P-2602HWUDL-D

802.11g Wireless ADSL VoIP IAD
with Built-in DECT Base Station

User's Guide

Version 3.40
8/2007
Edition 1

ZyXEL
www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.

It is recommended you use the web configurator to configure the ZyXEL Device.

- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

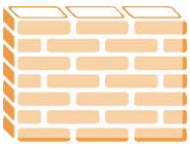
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-2602HWUDL-D may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router
DECT Phone	USB Hard Drive	

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.

Contents Overview

Introduction **41**

Introducing the ZyXEL Device 43
Tutorial 51
Introducing the Web Configurator 81

Wizard **89**

Internet and Wireless Setup Wizard 91
VoIP Wizard And Example 105
Bandwidth Management Wizard 111

Advanced **115**

Status Screens 117
WAN Setup 127
LAN Setup 143
Wireless LAN 155
Network Address Translation (NAT) Screens 173
Voice 185
VoIP Trunking 221
Phone Usage 237
Firewalls 241
Content Filtering 261
Introduction to IPSec 265
VPN Screens 271
Certificates 297
Static Route 321
Bandwidth Management 325
Dynamic DNS Setup 333
Remote Management Configuration 337
Universal Plug-and-Play (UPnP) 347
Sharing a USB Printer 359
File Sharing 377

Maintenance, Troubleshooting and Specifications **389**

System 391
Logs 395
Tools 409
Diagnostic 421

Troubleshooting 425
Product Specifications 433

Appendices and Index 445

Table of Contents

About This User's Guide **3**

Document Conventions **4**

Safety Warnings **6**

Contents Overview **9**

Table of Contents **11**

List of Figures **25**

List of Tables **35**

Part I: Introduction **41**

Chapter 1
Introducing the ZyXEL Device **43**

1.1 Overview 43
1.2 Ways to Manage the ZyXEL Device 44
1.3 Good Habits for Managing the ZyXEL Device 44
1.4 Applications for the ZyXEL Device 45
1.4.1 Internet Access 45
1.4.2 VoIP Features 46
1.4.3 VoIP Trunking Gateway 46
1.4.4 DECT Base Station Feature 47
1.4.5 ZyXEL Device's USB Support 47
1.5 LEDs (Lights) 48
1.6 The RESET Button 49
1.6.1 Using the Reset Button 49
1.7 The WLAN Button 50
1.7.1 Turn the Wireless LAN Off or On 50
1.7.2 Activate OTIST 50

Chapter 2
Tutorial **51**

2.1 How to Set up a Wireless Network 51
2.2 Example Parameters 51
2.3 Configuring the AP 51

2.4 Configuring the Wireless Client 53
2.4.1 Connecting to a Wireless LAN 54
2.4.2 Creating and Using a Profile 56
2.5 Using NAT with Multiple Public IP Addresses 58
2.5.1 Example Parameters and Scenario 59
2.5.2 Configuring the WAN Connection with a Static IP Address 59
2.5.3 Public IP Address Mapping 62
2.5.4 Forwarding Traffic from the WAN to a Local Computer 66
2.5.5 Allow WAN-to-LAN Traffic through the Firewall 67
2.5.6 Testing the Connections 73
2.6 Using NAT with Multiple Game Players 74
2.7 How to Make a VoIP Call 75
2.7.1 VoIP Calls With a Registered SIP Account 75
2.7.2 VoIP Calls Without a SIP Server 77

Chapter 3
Introducing the Web Configurator 81

3.1 Web Configurator Overview 81
3.1.1 Accessing the Web Configurator 81
3.2 Web Configurator Main Screen 84
3.2.1 Title Bar 84
3.2.2 Navigation Panel 85
3.2.3 Main Window 87
3.2.4 Status Bar 88

Part II: Wizard 89

Chapter 4
Internet and Wireless Setup Wizard 91

4.1 Introduction 91
4.2 Internet Access Wizard Setup 91
4.2.1 Manual Configuration 94
4.3 Wireless Connection Wizard Setup 99
4.3.1 Manually Assign a WPA key 102
4.3.2 Manually Assign a WEP Key 102

Chapter 5
VoIP Wizard And Example 105

5.1 Introduction 105
5.2 VoIP Wizard Setup 105

Chapter 6
Bandwidth Management Wizard 111

6.1 Introduction 111
6.2 Bandwidth Management Wizard Setup 111

Part III: Advanced 115

Chapter 7
Status Screens 117

7.1 Status Screen 117
7.2 Any IP Table 121
7.3 WLAN Status 122
7.4 Packet Statistics 122
7.5 VoIP Statistics 124

Chapter 8
WAN Setup 127

8.1 WAN Overview 127
8.1.1 Encapsulation 127
8.1.2 Multiplexing 128
8.1.3 VPI and VCI 128
8.1.4 IP Address Assignment 128
8.1.5 Nailed-Up Connection (PPP) 129
8.1.6 NAT 129
8.2 Metric 129
8.3 Traffic Shaping 130
8.3.1 ATM Traffic Classes 130
8.4 Zero Configuration Internet Access 131
8.5 Internet Access Setup 131
8.5.1 Advanced Internet Access Setup 134
8.6 WAN More Connections 135
8.6.1 More Connections Edit 136
8.6.2 Configuring More Connections Advanced Setup 139
8.7 Traffic Redirect 140
8.8 WAN Backup Setup 141

Chapter 9
LAN Setup 143

9.1 LAN Overview 143
9.1.1 LANs, WANs and the ZyXEL Device 143
9.1.2 DHCP Setup 143

9.2 DNS Server Addresses 144
9.3 LAN TCP/IP 144
9.3.1 IP Address and Subnet Mask 144
9.3.2 RIP Setup 145
9.3.3 Multicast 146
9.3.4 Any IP 146
9.4 Configuring LAN IP 148
9.4.1 Configuring Advanced LAN Setup 148
9.5 DHCP Setup 150
9.6 LAN Client List 151
9.7 LAN IP Alias 152

Chapter 10
Wireless LAN 155

10.1 Wireless Network Overview 155
10.2 Wireless Security Overview 156
10.2.1 SSID 156
10.2.2 MAC Address Filter 156
10.2.3 User Authentication 156
10.2.4 Encryption 157
10.2.5 One-Touch Intelligent Security Technology (OTIST) 158
10.3 Wireless Performance Overview 158
10.3.1 Quality of Service (QoS) 158
10.4 Additional Wireless Terms 158
10.5 General WLAN Screen 159
10.5.1 No Security 160
10.5.2 WEP Encryption Screen 160
10.5.3 WPA(2)-PSK 161
10.5.4 WPA(2) Authentication Screen 163
10.5.5 Wireless LAN Advanced Setup 164
10.6 OTIST Screen 165
10.6.1 Notes on OTIST 168
10.7 MAC Filter 168
10.8 QoS Screen 170
10.8.1 Application Priority Configuration 171

Chapter 11
Network Address Translation (NAT) Screens 173

11.1 NAT General Overview 173
11.1.1 NAT Definitions 173
11.1.2 What NAT Does 174
11.1.3 How NAT Works 174
11.1.4 NAT Application 175

11.1.5 NAT Mapping Types 175
11.2 SUA (Single User Account) Versus NAT 176
11.3 NAT General Setup 176
11.4 Port Forwarding 177
11.4.1 Default Server IP Address 178
11.4.2 Port Forwarding: Services and Port Numbers 178
11.4.3 Configuring Servers Behind Port Forwarding (Example) 178
11.5 Configuring Port Forwarding 179
11.5.1 Port Forwarding Rule Edit 180
11.6 Address Mapping 181
11.6.1 Address Mapping Rule Edit 182
11.6.2 SIP ALG 184

Chapter 12
Voice 185

12.1 Introduction to VoIP 185
12.2 SIP 185
12.2.1 SIP Identities 185
12.2.2 SIP Servers 186
12.2.3 RTP 188
12.2.4 Pulse Code Modulation 188
12.2.5 SIP Call Progression 188
12.2.6 SIP Call Progression Through Proxy Servers 189
12.2.7 Voice Coding 190
12.2.8 PSTN Call Setup Signaling 191
12.2.9 MWI (Message Waiting Indication) 191
12.2.10 Custom Tones (IVR) 191
12.3 Quality of Service (QoS) 192
12.3.1 Type of Service (ToS) 192
12.3.2 DiffServ 192
12.3.3 VLAN Tagging 193
12.4 SIP Settings Screen 193
12.5 Advanced SIP Setup Screen 195
12.6 SIP QoS Screen 199
12.7 Phone 199
12.7.1 Voice Activity Detection/Silence Suppression 199
12.7.2 Comfort Noise Generation 200
12.7.3 Echo Cancellation 200
12.8 Analog Phone Screen 200
12.9 Advanced Analog Phone Setup Screen 201
12.10 DECT Base Station Overview 202
12.10.1 DECT Phone Registration 203
12.10.2 Using your DECT Phone 205

12.10.3 DECT Phone Screen 206
12.11 Common Phone Settings Screen 208
12.12 Phone Services Overview 209
12.12.1 The Flash Key 209
12.12.2 Europe Type Supplementary Phone Services 209
12.12.3 USA Type Supplementary Services 211
12.13 Phone Region Screen 212
12.14 Speed Dial 213
12.15 Incoming Call Policy Screen 214
12.16 Distinctive Ring Screen 216
12.17 PSTN Line 218
12.18 PSTN Line Screen 218

Chapter 13
VoIP Trunking 221

13.1 VoIP Trunking Overview 221
13.2 VoIP Trunking and Security 221
13.2.1 Auto Attendant and Authentication 221
13.2.2 Peer Call Authentication 222
13.3 Call Rules 223
13.4 VoIP Trunking Scenarios 223
13.4.1 VoIP Phone To PSTN Phone 223
13.4.2 PSTN Phone To VoIP Phone 223
13.4.3 PSTN Phone To PSTN Phone via VoIP 224
13.5 Trunking General Screen 224
13.6 Trunking Peer Call Screen 225
13.7 Trunking Call Rule Screen 227
13.8 VoIP Trunking Example: VoIP to PSTN 229
13.8.1 Background Information 229
13.8.2 Configuration Details: Outgoing 229
13.8.3 Configuration Details: Incoming 230
13.8.4 Call Progression 231
13.9 VoIP Trunking Example: PSTN to PSTN via VoIP 231
13.9.1 Background Information 232
13.9.2 Configuration Details: Outgoing 232
13.9.3 Configuration Details: Incoming 234
13.9.4 Call Progression 234

Chapter 14
Phone Usage 237

14.1 Dialing a Telephone Number 237
14.2 Using Speed Dial to Dial a Telephone Number 237
14.3 Internal Calls 237

14.4 Using Call Park and Pickup 237
14.5 Checking the ZyXEL Device's IP Address 238
14.6 Auto Provisioning and Auto Firmware Upgrade 238
14.7 Phone Functions Summary 238

Chapter 15
Firewalls 241

15.1 Firewall Overview 241
15.1.1 Stateful Inspection Firewall 241
15.1.2 About the ZyXEL Device Firewall 241
15.1.3 Guidelines For Enhancing Security With Your Firewall 242
15.2 General Firewall Policy Overview 242
15.3 Security Considerations 244
15.4 Triangle Route 244
15.4.1 The "Triangle Route" Problem 245
15.4.2 Solving the "Triangle Route" Problem 245
15.5 General Firewall Policy 246
15.6 Firewall Rules Summary 247
15.6.1 Configuring Firewall Rules 249
15.6.2 Customized Services 252
15.6.3 Configuring A Customized Service 252
15.7 Example Firewall Rule 253
15.8 Firewall Thresholds 257
15.8.1 Threshold Values 258
15.8.2 Configuring Firewall Thresholds 258

Chapter 16
Content Filtering 261

16.1 Content Filtering Overview 261
16.2 Configuring Keyword Blocking 261
16.3 Configuring the Schedule 262
16.4 Configuring Trusted Computers 263

Chapter 17
Introduction to IPSec 265

17.1 VPN Overview 265
17.1.1 IPSec 265
17.1.2 Security Association 265
17.1.3 Other Terminology 265
17.1.4 VPN Applications 266
17.2 IPSec Architecture 266
17.2.1 IPSec Algorithms 267
17.2.2 Key Management 267

17.3 Encapsulation 267
17.3.1 Transport Mode 268
17.3.2 Tunnel Mode 268
17.4 IPSec and NAT 268

Chapter 18
VPN Screens 271

18.1 VPN/IPSec Overview 271
18.2 IPSec Algorithms 271
18.2.1 AH (Authentication Header) Protocol 271
18.2.2 ESP (Encapsulating Security Payload) Protocol 271
18.3 My IP Address 272
18.4 Secure Gateway Address 272
18.4.1 Dynamic Secure Gateway Address 273
18.5 VPN Setup Screen 273
18.6 Keep Alive 275
18.7 VPN, NAT, and NAT Traversal 275
18.8 Remote DNS Server 276
18.9 ID Type and Content 277
18.9.1 ID Type and Content Examples 278
18.10 Pre-Shared Key 279
18.11 Editing VPN Policies 279
18.12 IKE Phases 284
18.12.1 Negotiation Mode 285
18.12.2 Diffie-Hellman (DH) Key Groups 285
18.12.3 Perfect Forward Secrecy (PFS) 285
18.13 Configuring Advanced IKE Settings 285
18.14 Manual Key Setup 288
18.14.1 Security Parameter Index (SPI) 288
18.15 Configuring Manual Key 288
18.16 Viewing SA Monitor 291
18.17 Configuring VPN Global Setting 293
18.18 Telecommuter VPN/IPSec Examples 293
18.18.1 Telecommuters Sharing One VPN Rule Example 293
18.18.2 Telecommuters Using Unique VPN Rules Example 294
18.19 VPN and Remote Management 296

Chapter 19
Certificates 297

19.1 Certificates Overview 297
19.1.1 Advantages of Certificates 298
19.2 Self-signed Certificates 298
19.3 Configuration Summary 298

19.4 My Certificates 298
19.5 My Certificate Import 300
19.5.1 Certificate File Formats 301
19.6 My Certificate Create 302
19.7 My Certificate Details 304
19.8 Trusted CAs 307
19.9 Trusted CA Import 309
19.10 Trusted CA Details 310
19.11 Trusted Remote Hosts 312
19.12 Verifying a Trusted Remote Host's Certificate 314
19.12.1 Trusted Remote Host Certificate Fingerprints 314
19.13 Trusted Remote Hosts Import 315
19.14 Trusted Remote Host Certificate Details 315
19.15 Directory Servers 318
19.16 Directory Server Add and Edit 319

Chapter 20
Static Route 321

20.1 Static Route 321
20.2 Configuring Static Route 321
20.2.1 Static Route Edit 322

Chapter 21
Bandwidth Management 325

21.1 Bandwidth Management Overview 325
21.2 Application-based Bandwidth Management 325
21.3 Auto Classifier 325
21.4 Subnet-based Bandwidth Management 326
21.5 Application and Subnet-based Bandwidth Management 327
21.5.1 Bandwidth Management Priorities 327
21.6 Configuring Bandwidth Management (General) 327
21.7 Bandwidth Management Rule Setup 328
21.7.1 Rule Configuration 329
21.8 Bandwidth Monitor 332

Chapter 22
Dynamic DNS Setup 333

22.1 Dynamic DNS Overview 333
22.1.1 DYNDNS Wildcard 333
22.2 Configuring Dynamic DNS 333

Chapter 23
Remote Management Configuration 337

23.1 Remote Management Overview 337
23.1.1 Remote Management Limitations 338
23.1.2 Remote Management and NAT 338
23.1.3 System Timeout 338
23.2 WWW 338
23.3 Telnet 339
23.4 Configuring Telnet 339
23.5 Configuring FTP 340
23.6 SNMP 341
23.6.1 Supported MIBs 342
23.6.2 SNMP Traps 343
23.6.3 Configuring SNMP 343
23.7 Configuring DNS 344
23.8 Configuring ICMP 345

Chapter 24
Universal Plug-and-Play (UPnP) 347

24.1 Introducing Universal Plug and Play 347
24.1.1 How do I know if I'm using UPnP? 347
24.1.2 NAT Traversal 347
24.1.3 Cautions with UPnP 347
24.2 UPnP and ZyXEL 348
24.2.1 Configuring UPnP 348
24.3 Installing UPnP in Windows Example 349
24.4 Using UPnP in Windows XP Example 352

Chapter 25
Sharing a USB Printer 359

25.1 Overview 359
25.2 Requirements 359
25.3 Configure a TCP/IP Printer Port 360
25.4 Print Server Screen 364
25.5 Adding a New Printer Example 365
25.6 Macintosh OS X Adding Printer Example 370
25.7 ZyXEL Device Print Server Compatible USB Printers 373

Chapter 26
File Sharing 377

26.1 File Sharing Implementation Overview 377
26.2 Sharing Files via the ZyXEL Device 378
26.2.1 Using the Workgroup Name to Share Files 378
26.3 User Accounts 379
26.4 File Sharing - Server Configuration 379

26.5 User Configuration 380
26.5.1 Add or Edit a User Account 381
26.6 Share Configuration 382
26.6.1 Default Share Directory List 382
26.6.2 User-Defined Share Directory List 383
26.6.3 Add or Edit a User-Defined Share 383
26.6.4 Browse 384
26.7 Examples of Accessing Files via the ZyXEL Device 385
26.7.1 Using Windows Explorer to Share Files 385
26.7.2 Using the Run Utility to Share Files 386
26.7.3 Using FTP to Share Files 386
26.7.4 Using the Workgroup Name to Access Files 387

Part IV: Maintenance, Troubleshooting and Specifications 389

Chapter 27
System 391

27.1 General Setup and System Name 391
27.1.1 General Setup 391
27.2 Time Setting 393

Chapter 28
Logs 395

28.1 Logs Overview 395
28.1.1 Alerts and Logs 395
28.2 Viewing the Logs 395
28.3 Configuring Log Settings 396
28.4 SMTP Error Messages 398
28.4.1 Example E-mail Log 399
28.5 Log Descriptions 400

Chapter 29
Tools 409

29.1 Introduction 409
29.2 Filename Conventions 409
29.3 FTP Restrictions 410
29.4 Firmware Upgrade Screen 410
29.5 Backup and Restore 412
29.5.1 Backup Configuration 413
29.5.2 Restore Configuration 413
29.5.3 Reset to Factory Defaults 414

29.6 Restart 415
29.7 Using FTP or TFTP to Back Up Configuration 415
29.7.1 Using the FTP Commands to Back Up Configuration 415
29.7.2 FTP Command Configuration Backup Example 416
29.7.3 Configuration Backup Using GUI-based FTP Clients 416
29.7.4 Backup Configuration Using TFTP 417
29.7.5 TFTP Command Configuration Backup Example 417
29.7.6 Configuration Backup Using GUI-based TFTP Clients 417
29.8 Using FTP or TFTP to Restore Configuration 418
29.8.1 Restore Using FTP Session Example 418
29.9 FTP and TFTP Firmware and Configuration File Uploads 418
29.9.1 FTP File Upload Command from the DOS Prompt Example 419
29.9.2 FTP Session Example of Firmware File Upload 419
29.9.3 TFTP File Upload 420
29.9.4 TFTP Upload Command Example 420

Chapter 30
Diagnostic 421

30.1 General Diagnostic 421
30.2 DSL Line Diagnostic 421

Chapter 31
Troubleshooting 425

31.1 Power, Hardware Connections, and LEDs 425
31.2 ZyXEL Device Access and Login 426
31.3 Internet Access 428
31.4 Phone Calls and VoIP 429
31.5 Multiple SIP Accounts 429
31.5.1 Outgoing Calls 429
31.5.2 Incoming Calls 430
31.6 USB Device Connection 431

Chapter 32
Product Specifications 433

Part V: Appendices and Index 445

Appendix A Setting up Your Computer's IP Address 447

Appendix B Pop-up Windows, JavaScripts and Java Permissions 469

Appendix C IP Addresses and Subnetting 477

Appendix D Wireless LANs 485

Appendix E Services 499
Appendix F Internal SPTGEN 503
Appendix G Legal Information 527
Appendix H Customer Support 531
Index 537

List of Figures

Figure 1 ZyXEL Device's Router Features 45
Figure 2 ZyXEL Device's VoIP Features 46
Figure 3 ZyXEL Device as a VoIP Trunking Gateway 46
Figure 4 DECT Base Station Feature 47
Figure 5 File Sharing Overview 47
Figure 6 LEDs on the Top of the Device 48
Figure 7 AP: Wireless LAN > General 52
Figure 8 AP: Wireless LAN > General > Advanced Setup 52
Figure 9 AP: Status 53
Figure 10 AP: Status: WLAN Station Status 53
Figure 11 ZyXEL Utility: Site Survey 54
Figure 12 ZyXEL Utility: Security Settings 55
Figure 13 ZyXEL Utility: Confirm Save 55
Figure 14 ZyXEL Utility: Link Info 55
Figure 15 ZyXEL Utility: Profile 56
Figure 16 ZyXEL Utility: Add New Profile 56
Figure 17 ZyXEL Utility: Profile Security 57
Figure 18 ZyXEL Utility: Profile Encryption 57
Figure 19 Profile: Wireless Protocol Settings. 57
Figure 20 Profile: Confirm Save 58
Figure 21 Profile: Activate 58
Figure 22 Tutorial Example: Using NAT with Static Public IP Addresses 59
Figure 23 Tutorial Example: WAN Connection with a Static Public IP Address 60
Figure 24 Tutorial Example: WAN Screen 61
Figure 25 Tutorial Example: Status 62
Figure 26 Tutorial Example: Mapping Multiple Public IP Addresses to Inside Servers 63
Figure 27 Tutorial Example: NAT > NAT Overview 63
Figure 28 Tutorial Example: NAT > Address Mapping 64
Figure 29 Tutorial Example: NAT Address Mapping Edit: One-to-One (1) 64
Figure 30 Tutorial Example: NAT Address Mapping Edit: One-to-One (2) 65
Figure 31 Tutorial Example: NAT Address Mapping Edit: Many-to-One 65
Figure 32 Tutorial Example: NAT Address Mapping Done 66
Figure 33 Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer 66
Figure 34 Tutorial Example: NAT Address Mapping Edit: Server 67
Figure 35 Tutorial Example: NAT Port Forwarding 67
Figure 36 Tutorial Example: Allow WAN-to-LAN Traffic 68
Figure 37 Tutorial Example: Firewall > General 68
Figure 38 Tutorial Example: Firewall Rules: WAN to LAN 69

Figure 39 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Web Server 69
Figure 40 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Web Server 70
Figure 41 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Mail Server 71
Figure 42 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Mail Server 71
Figure 43 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for FTP Server 72
Figure 44 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for FTP Server 73
Figure 45 Tutorial Example: Firewall Rules Done 73
Figure 46 Tutorial Example: NAT Address Mapping Done: Game Playing 74
Figure 47 Tutorial Example: SIP Settings 76
Figure 48 Tutorial Example: Status 76
Figure 49 Tutorial Example: Analog Phone 77
Figure 50 Tutorial Example: SIP Settings for an Unregistered SIP Account 78
Figure 51 Tutorial Example: Analog Phone 79
Figure 52 Tutorial Example: Speed Dial 80
Figure 53 Password Screen 82
Figure 54 Change Password Screen 82
Figure 55 Replace Certificate Screen 83
Figure 56 Wizard or Advanced Screen 83
Figure 57 Main Screen 84
Figure 58 Select a Mode 92
Figure 59 Wizard Welcome 92
Figure 60 Auto Detection: No DSL Connection 93
Figure 61 Auto-Detection: PPPoE 93
Figure 62 Auto Detection: Failed 94
Figure 63 Internet Access Wizard Setup: ISP Parameters 95
Figure 64 Internet Connection with PPPoE 96
Figure 65 Internet Connection with RFC 1483 96
Figure 66 Internet Connection with ENET ENCAP 97
Figure 67 Internet Connection with PPPoA 98
Figure 68 Connection Test Failed-1 99
Figure 69 Connection Test Failed-2. 99
Figure 70 Connection Test Successful 100
Figure 71 Wireless LAN Setup Wizard 1 100
Figure 72 Wireless LAN 101
Figure 73 Manually Assign a WPA key 102
Figure 74 Manually Assign a WEP key 102
Figure 75 Wireless LAN Setup 3 103
Figure 76 Internet Access and WLAN Wizard Setup Complete 104
Figure 77 VoIP Phone Calls 105
Figure 78 Select a Mode 106
Figure 79 Wizard: Welcome 106
Figure 80 VoIP Wizard Configuration 107
Figure 81 SIP Registration Test 108

Figure 82 VoIP Wizard Fail 108
Figure 83 VoIP Wizard Finish 109
Figure 84 Select a Mode 111
Figure 85 Wizard: Welcome 112
Figure 86 Bandwidth Management Wizard: General Information 112
Figure 87 Bandwidth Management Wizard: Complete 113
Figure 88 Status Screen 118
Figure 89 Any IP Table 121
Figure 90 WLAN Status 122
Figure 91 Packet Statistics 123
Figure 92 VoIP Statistics 124
Figure 93 Example of Traffic Shaping 130
Figure 94 Internet Access Setup (PPPoE) 132
Figure 95 Advanced Internet Access Setup 134
Figure 96 WAN More Connections 135
Figure 97 More Connections Edit 137
Figure 98 More Connections Advanced Setup 139
Figure 99 Traffic Redirect Example 140
Figure 100 Traffic Redirect LAN Setup 140
Figure 101 WAN Backup Setup 141
Figure 102 LAN and WAN IP Addresses 143
Figure 103 Any IP Example 147
Figure 104 LAN IP 148
Figure 105 Advanced LAN Setup 149
Figure 106 DHCP Setup 150
Figure 107 LAN Client List 151
Figure 108 Physical Network & Partitioned Logical Networks 153
Figure 109 LAN IP Alias 153
Figure 110 Example of a Wireless Network 155
Figure 111 Wireless LAN: General 159
Figure 112 Wireless: No Security 160
Figure 113 Wireless: Static WEP Encryption 161
Figure 114 Wireless: WPA(2)-PSK 162
Figure 115 Wireless: WPA(2) 163
Figure 116 Advanced 164
Figure 117 Network > Wireless LAN > OTIST 166
Figure 118 Example: Wireless Client OTIST Screen 167
Figure 119 OTIST: Settings 167
Figure 120 OTIST: In Progress on the ZyXEL Device 167
Figure 121 OTIST: In Progress on the Wireless Device 168
Figure 122 Start OTIST? 168
Figure 123 MAC Address Filter 169
Figure 124 Wireless LAN: QoS 170

Figure 125 Application Priority Configuration 171
Figure 126 How NAT Works 174
Figure 127 NAT Application With IP Alias 175
Figure 128 NAT General 177
Figure 129 Multiple Servers Behind NAT Example 179
Figure 130 Port Forwarding 179
Figure 131 Port Forwarding Rule Setup 180
Figure 132 Address Mapping Rules 182
Figure 133 Edit Address Mapping Rule 183
Figure 134 Network > NAT > ALG 184
Figure 135 SIP User Agent 187
Figure 136 SIP Proxy Server 187
Figure 137 SIP Redirect Server 188
Figure 138 SIP Call Through Proxy Servers 189
Figure 139 DiffServ: Differentiated Service Field 193
Figure 140 SIP > SIP Settings 194
Figure 141 VoIP > SIP Settings > Advanced 196
Figure 142 SIP > QoS 199
Figure 143 Phone > Analog Phone 200
Figure 144 Phone > Analog Phone > Advanced 201
Figure 145 DECT Base Station Overview 203
Figure 146 DECT Base Station Button - Side of the ZyXEL Device 204
Figure 147 DECT Base Station - Phone Registration 204
Figure 148 Using Your DECT Phone 205
Figure 149 VoIP > Phone > DECT Phone 207
Figure 150 Phone > Common 208
Figure 151 VoIP > Phone > Region 212
Figure 152 Phone Book > Speed Dial 213
Figure 153 Phone Book > Incoming Call Policy 215
Figure 154 Phone Book > Distinctive Ring 217
Figure 155 PSTN Line > General 219
Figure 156 Peer Devices Connecting 222
Figure 157 VoIP Phone To PSTN Phone 223
Figure 158 PSTN Phone To VoIP Phone 224
Figure 159 PSTN Phone To PSTN Phone via VoIP 224
Figure 160 VoIP > Trunking > General 225
Figure 161 VoIP > Trunking > Peer Call 226
Figure 162 VoIP > Trunking > Call Rule 228
Figure 163 VoIP to PSTN Example 229
Figure 164 VoIP to PSTN Example - Speed Dial Screen 230
Figure 165 VoIP to PSTN Example - Outgoing Authentication 230
Figure 166 VoIP to PSTN Example - Incoming Authentication 231
Figure 167 PSTN to PSTN Example 232

Figure 168 PSTN to PSTN Example: General Configuration 233
Figure 169 PSTN to PSTN Example - Outgoing Authentication From Device B 233
Figure 170 PSTN to PSTN Example - Call Rule 234
Figure 171 PSTN to PSTN Example - Incoming Authentication To Device C 234
Figure 172 Default Firewall Action 242
Figure 173 Ideal Firewall Setup 244
Figure 174 “Triangle Route” Problem 245
Figure 175 IP Alias 246
Figure 176 Firewall: General 246
Figure 177 Firewall Rules 248
Figure 178 Firewall: Edit Rule 250
Figure 179 Firewall: Customized Services 252
Figure 180 Firewall: Configure Customized Services 253
Figure 181 Firewall Example: Rules 254
Figure 182 Edit Custom Port Example 254
Figure 183 Firewall Example: Edit Rule: Destination Address 255
Figure 184 Firewall Example: Edit Rule: Select Customized Services 256
Figure 185 Firewall Example: Rules: MyService 257
Figure 186 Three-Way Handshake 257
Figure 187 Firewall: Threshold 258
Figure 188 Content Filter: Keyword 261
Figure 189 Content Filter: Schedule 262
Figure 190 Content Filter: Trusted 263
Figure 191 Encryption and Decryption 266
Figure 192 IPSec Architecture 267
Figure 193 Transport and Tunnel Mode IPSec Encapsulation 268
Figure 194 IPSec Summary Fields 273
Figure 195 VPN Setup 274
Figure 196 NAT Router Between IPSec Routers 276
Figure 197 VPN Host using Intranet DNS Server Example 277
Figure 198 VPN Setup: Edit 280
Figure 199 Two Phases to Set Up the IPSec SA 284
Figure 200 Advanced VPN IKE 286
Figure 201 VPN Setup: Manual Key 289
Figure 202 VPN: SA Monitor 292
Figure 203 VPN: Global Setting 293
Figure 204 Telecommuters Sharing One VPN Rule Example 294
Figure 205 Telecommuters Using Unique VPN Rules Example 295
Figure 206 Certificate Configuration Overview 298
Figure 207 My Certificates 299
Figure 208 My Certificate Import 301
Figure 209 My Certificate Create 302
Figure 210 My Certificate Details 305

Figure 211 Trusted CAs 308
Figure 212 Trusted CA Import 309
Figure 213 Trusted CA Details 310
Figure 214 Trusted Remote Hosts 313
Figure 215 Remote Host Certificates 314
Figure 216 Certificate Details 314
Figure 217 Trusted Remote Host Import 315
Figure 218 Trusted Remote Host Details 316
Figure 219 Directory Servers 318
Figure 220 Directory Server Add and Edit 319
Figure 221 Example of Static Routing Topology 321
Figure 222 Static Route 322
Figure 223 Static Route Edit 323
Figure 224 Subnet-based Bandwidth Management Example 326
Figure 225 Bandwidth Management: General 327
Figure 226 Bandwidth Management: Rule Setup 328
Figure 227 Bandwidth Management Rule Configuration 330
Figure 228 Bandwidth Management: Monitor 332
Figure 229 Dynamic DNS 334
Figure 230 Remote Management From the WAN 337
Figure 231 Remote Management: WWW 339
Figure 232 Remote Management: Telnet 340
Figure 233 Remote Management: FTP 341
Figure 234 SNMP Management Model 342
Figure 235 Remote Management: SNMP 343
Figure 236 Remote Management: DNS 345
Figure 237 Remote Management: ICMP 346
Figure 238 Configuring UPnP 348
Figure 239 Add/Remove Programs: Windows Setup: Communication 349
Figure 240 Add/Remove Programs: Windows Setup: Communication: Components 350
Figure 241 Network Connections 350
Figure 242 Windows Optional Networking Components Wizard 351
Figure 243 Networking Services 351
Figure 244 Network Connections 352
Figure 245 Internet Connection Properties 353
Figure 246 Internet Connection Properties: Advanced Settings 354
Figure 247 Internet Connection Properties: Advanced Settings: Add 354
Figure 248 System Tray Icon 355
Figure 249 Internet Connection Status 355
Figure 250 Network Connections 356
Figure 251 Network Connections: My Network Places 357
Figure 252 Network Connections: My Network Places: Properties: Example 357
Figure 253 Sharing a USB Printer 359

Figure 254 Open Printers Window 360
Figure 255 Open Printer Properties 361
Figure 256 Printer Properties Window 361
Figure 257 Add a Port Window 361
Figure 258 Add a Port Wizard 362
Figure 259 Enter IP Address of the ZyXEL Device 362
Figure 260 Custom Port Settings 363
Figure 261 Custom Port Settings 363
Figure 262 Finish Adding the TCP/IP Port 364
Figure 263 Configuring Print Server 364
Figure 264 Printers Folder 365
Figure 265 Add Printer Wizard: Welcome 366
Figure 266 Add Printer Wizard: Local or Network Printer 366
Figure 267 Add Printer Wizard: Select the Printer Port 367
Figure 268 Add Printer Wizard: Printer Driver 367
Figure 269 Add Printer Wizard: Use Existing Driver 368
Figure 270 Add Printer Wizard: Name Your Printer 368
Figure 271 Add Printer Wizard: Printer Sharing 369
Figure 272 Add Printer Wizard: Print Test Page 369
Figure 273 Add Printer Wizard Complete 370
Figure 274 Macintosh HD 370
Figure 275 Macintosh HD folder 370
Figure 276 Applications Folder 371
Figure 277 Utilities Folder 371
Figure 278 Printer List Folder 371
Figure 279 Printer Configuration 372
Figure 280 Printer Model 372
Figure 281 Print Server 372
Figure 282 File Sharing Overview 377
Figure 283 Check the Workgroup Name 379
Figure 284 File Sharing Login 379
Figure 285 File Sharing > Server Configuration 380
Figure 286 File Sharing > User Configuration 381
Figure 287 File Sharing > User Configuration > Add/Edit 381
Figure 288 File Sharing > Share Configuration: Default 382
Figure 289 File Sharing > Share Configuration: User-Defined 383
Figure 290 File Sharing > Share Configuration: User-Defined > Add/Edit 383
Figure 291 File Sharing > Share Configuration: User-Defined > Browse 384
Figure 292 File Sharing via Windows Explorer 385
Figure 293 Run Utility to Browse Files 386
Figure 294 File Sharing via FTP: Address 386
Figure 295 File Sharing via FTP: Login 386
Figure 296 File Sharing via FTP: Login 387

Figure 297 Browse to a File Share via Workgroup Name 388
Figure 298 System General Setup 392
Figure 299 System Time Setting 393
Figure 300 View Log 396
Figure 301 Log Settings 397
Figure 302 E-mail Log Example 399
Figure 303 Firmware Upgrade 411
Figure 304 Firmware Upload In Progress 411
Figure 305 Network Temporarily Disconnected 412
Figure 306 Error Message 412
Figure 307 Configuration 413
Figure 308 Configuration Upload Successful 414
Figure 309 Network Temporarily Disconnected 414
Figure 310 Configuration Upload Error 414
Figure 311 Reset Warning Message 415
Figure 312 Reset In Process Message 415
Figure 313 Restart Screen 415
Figure 314 FTP Session Example 416
Figure 315 Restore Using FTP Session Example 418
Figure 316 FTP Session Example of Firmware File Upload 419
Figure 317 Diagnostic: General 421
Figure 318 Diagnostic: DSL Line 422
Figure 319 Outgoing Calls: Default 430
Figure 320 Outgoing Calls: Individual Configuration 430
Figure 321 Incoming Calls: Default 431
Figure 322 Incoming Calls: Individual Configuration 431
Figure 323 WIndows 95/98/Me: Network: Configuration 448
Figure 324 Windows 95/98/Me: TCP/IP Properties: IP Address 449
Figure 325 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 450
Figure 326 Windows XP: Start Menu 451
Figure 327 Windows XP: Control Panel 451
Figure 328 Windows XP: Control Panel: Network Connections: Properties 452
Figure 329 Windows XP: Local Area Connection Properties 452
Figure 330 Windows XP: Internet Protocol (TCP/IP) Properties 453
Figure 331 Windows XP: Advanced TCP/IP Properties 454
Figure 332 Windows XP: Internet Protocol (TCP/IP) Properties 455
Figure 333 Windows Vista: Start Menu 456
Figure 334 Windows Vista: Control Panel 456
Figure 335 Windows Vista: Network And Internet 456
Figure 336 Windows Vista: Network and Sharing Center 456
Figure 337 Windows Vista: Network and Sharing Center 457
Figure 338 Windows Vista: Local Area Connection Properties 457
Figure 339 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties 458

Figure 340 Windows Vista: Advanced TCP/IP Properties 459
Figure 341 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties 460
Figure 342 Macintosh OS 8/9: Apple Menu 461
Figure 343 Macintosh OS 8/9: TCP/IP 461
Figure 344 Macintosh OS X: Apple Menu 462
Figure 345 Macintosh OS X: Network 463
Figure 346 Red Hat 9.0: KDE: Network Configuration: Devices 464
Figure 347 Red Hat 9.0: KDE: Ethernet Device: General 464
Figure 348 Red Hat 9.0: KDE: Network Configuration: DNS 465
Figure 349 Red Hat 9.0: KDE: Network Configuration: Activate 465
Figure 350 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 466
Figure 351 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 466
Figure 352 Red Hat 9.0: DNS Settings in resolv.conf 466
Figure 353 Red Hat 9.0: Restart Ethernet Card 466
Figure 354 Red Hat 9.0: Checking TCP/IP Properties 467
Figure 355 Pop-up Blocker 469
Figure 356 Internet Options: Privacy 470
Figure 357 Internet Options: Privacy 471
Figure 358 Pop-up Blocker Settings 471
Figure 359 Internet Options: Security 472
Figure 360 Security Settings - Java Scripting 473
Figure 361 Security Settings - Java 473
Figure 362 Java (Sun) 474
Figure 363 Mozilla Firefox: Tools > Options 475
Figure 364 Mozilla Firefox Content Security 475
Figure 365 Network Number and Host ID 478
Figure 366 Subnetting Example: Before Subnetting 480
Figure 367 Subnetting Example: After Subnetting 481
Figure 368 Peer-to-Peer Communication in an Ad-hoc Network 485
Figure 369 Basic Service Set 486
Figure 370 Infrastructure WLAN 487
Figure 371 RTS/CTS 488
Figure 372 WPA(2) with RADIUS Application Example 495
Figure 373 WPA(2)-PSK Authentication 496
Figure 374 Configuration Text File Format: Column Descriptions 503
Figure 375 Invalid Parameter Entered: Command Line Example 504
Figure 376 Valid Parameter Entered: Command Line Example 504
Figure 377 Internal SPTGEN FTP Download Example 505
Figure 378 Internal SPTGEN FTP Upload Example 505

List of Tables

Table 1 Models Covered 43
Table 2 LED Descriptions 48
Table 3 Web Configurator Icons in the Title Bar 84
Table 4 Navigation Panel Summary 85
Table 5 Internet Access Wizard Setup: ISP Parameters 95
Table 6 Internet Connection with PPPoE 96
Table 7 Internet Connection with RFC 1483 97
Table 8 Internet Connection with ENET ENCAP 97
Table 9 Internet Connection with PPPoA 98
Table 10 Wireless LAN Setup Wizard 1 100
Table 11 Wireless LAN Setup Wizard 2 101
Table 12 Manually Assign a WPA key 102
Table 13 Manually Assign a WEP key 103
Table 14 Sample SIP Account Information 106
Table 15 VoIP Wizard Configuration 107
Table 16 Bandwidth Management Wizard: General Information 112
Table 17 Status Screen 118
Table 18 Any IP Table 121
Table 19 WLAN Status 122
Table 20 Packet Statistics 123
Table 21 VoIP Statistics 125
Table 22 Internet Access Setup 132
Table 23 Advanced Internet Access Setup 134
Table 24 Advanced Internet Access Setup 136
Table 25 More Connections Edit 137
Table 26 More Connections Advanced Setup 139
Table 27 WAN Backup Setup 141
Table 28 LAN IP 148
Table 29 Advanced LAN Setup 149
Table 30 DHCP Setup 150
Table 31 LAN Client List 152
Table 32 LAN IP Alias 153
Table 33 Types of Encryption for Each Type of Authentication 157
Table 34 Additional Wireless Terms 158
Table 35 Wireless LAN: General 159
Table 36 Wireless No Security 160
Table 37 Wireless: Static WEP Encryption 161
Table 38 Wireless: WPA(2)-PSK 162

Table 39 Wireless: WPA(2) 163
Table 40 Wireless LAN: Advanced 165
Table 41 Network > Wireless LAN > OTIST 166
Table 42 MAC Address Filter 169
Table 43 Wireless LAN: QoS 170
Table 44 Application Priority Configuration 171
Table 45 NAT Definitions 173
Table 46 NAT Mapping Types 176
Table 47 NAT General 177
Table 48 Port Forwarding 180
Table 49 Port Forwarding Rule Setup 181
Table 50 Address Mapping Rules 182
Table 51 Edit Address Mapping Rule 183
Table 52 Network > NAT > ALG 184
Table 53 SIP Call Progression 188
Table 54 SIP Call Progression 190
Table 55 Custom Tones Details 191
Table 56 SIP > SIP Settings 194
Table 57 VoIP > SIP Settings > Advanced 196
Table 58 SIP > QoS 199
Table 59 Phone > Analog Phone 200
Table 60 Phone > Analog Phone > Advanced 202
Table 61 DECT Phone Calls Summary 206
Table 62 VoIP > Phone > DECT Phone 207
Table 63 Phone > Common 208
Table 64 European Flash Key Commands 209
Table 65 USA Flash Key Commands 211
Table 66 VoIP > Phone > Region 212
Table 67 Phone Book > Speed Dial 213
Table 68 Phone Book > Incoming Call Policy 215
Table 69 Phone Book > Distinctive Ring 217
Table 70 PSTN Line > General 219
Table 71 Matching Incoming and Outgoing Authentication 222
Table 72 Call Rules 223
Table 73 VoIP > Trunking > General 225
Table 74 VoIP > Trunking > Peer Call 226
Table 75 VoIP > Trunking > Call Rule 228
Table 76 VoIP Trunking Call Progression 231
Table 77 PSTN to PSTN: VoIP Trunking Call Progression 235
Table 78 Phone Functions Summary 238
Table 79 Firewall: General 247
Table 80 Firewall Rules 248
Table 81 Firewall: Edit Rule 250

Table 82 Customized Services 252
Table 83 Firewall: Configure Customized Services 253
Table 84 Firewall: Threshold 259
Table 85 Content Filter: Keyword 262
Table 86 Content Filter: Schedule 263
Table 87 Content Filter: Trusted 263
Table 88 VPN and NAT 269
Table 89 AH and ESP 272
Table 90 VPN Setup 274
Table 91 VPN and NAT 276
Table 92 Local ID Type and Content Fields 278
Table 93 Peer ID Type and Content Fields 278
Table 94 Matching ID Type and Content Configuration Example 278
Table 95 Mismatching ID Type and Content Configuration Example 279
Table 96 VPN Setup; Edit 280
Table 97 Advanced VPN IKE 286
Table 98 VPN Setup: Manual Key 289
Table 99 VPN: SA Monitor 292
Table 100 VPN: Global Setting 293
Table 101 Telecommuters Sharing One VPN Rule Example 294
Table 102 Telecommuters Using Unique VPN Rules Example 295
Table 103 My Certificates 299
Table 104 My Certificate Import 301
Table 105 My Certificate Create 302
Table 106 My Certificate Details 306
Table 107 Trusted CAs 308
Table 108 Trusted CA Import 309
Table 109 Trusted CA Details 311
Table 110 Trusted Remote Hosts 313
Table 111 Trusted Remote Host Import 315
Table 112 Trusted Remote Host Details 316
Table 113 Directory Servers 319
Table 114 Directory Server Add and Edit 319
Table 115 Static Route 322
Table 116 Static Route Edit 323
Table 117 Typical Packet Sizes 326
Table 118 Automatic Traffic Classifier Priorities 326
Table 119 Application and Subnet-based Bandwidth Management Example 327
Table 120 Bandwidth Management Priorities 327
Table 121 Bandwidth Management: General 328
Table 122 Bandwidth Management: Rule Setup 328
Table 123 Bandwidth Management Rule Configuration 330
Table 124 Dynamic DNS 334

Table 125 Remote Management: WWW 339
Table 126 Remote Management: Telnet 340
Table 127 Remote Management: FTP 341
Table 128 SNMP Traps 343
Table 129 Remote Management: SNMP 344
Table 130 Remote Management: DNS 345
Table 131 Remote Management: ICMP 346
Table 132 Configuring UPnP 348
Table 133 Configuring Print Server 365
Table 134 Compatible USB Printers 373
Table 135 File Sharing > Server Configuration 380
Table 136 File Sharing > User Configuration 381
Table 137 File Sharing > User Configuration > Add/Edit 381
Table 138 File Sharing > Share Configuration: Default 382
Table 139 File Sharing > Share Configuration: User-Defined 383
Table 140 File Sharing > Share Configuration: User-Defined > Add/Edit 383
Table 141 File Sharing > Share Configuration: User-Defined > Browse 384
Table 142 System General Setup 392
Table 143 System Time Setting 393
Table 144 View Log 396
Table 145 Log Settings 397
Table 146 SMTP Error Messages 399
Table 147 System Maintenance Logs 400
Table 148 System Error Logs 401
Table 149 Access Control Logs 401
Table 150 TCP Reset Logs 401
Table 151 Packet Filter Logs 402
Table 152 ICMP Logs 402
Table 153 CDR Logs 402
Table 154 PPP Logs 403
Table 155 UPnP Logs 403
Table 156 Content Filtering Logs 403
Table 157 Attack Logs 403
Table 158 802.1X Logs 404
Table 159 ACL Setting Notes 405
Table 160 ICMP Notes 405
Table 161 Syslog Logs 406
Table 162 SIP Logs 406
Table 163 RTP Logs 406
Table 164 FSM Logs: Caller Side 407
Table 165 FSM Logs: Callee Side 407
Table 166 PSTN Logs 407
Table 167 RFC-2408 ISAKMP Payload Types 407

Table 168 Filename Conventions 410
Table 169 Firmware Upgrade 411
Table 170 Restore Configuration 413
Table 171 General Commands for GUI-based FTP Clients 416
Table 172 General Commands for GUI-based TFTP Clients 417
Table 173 Diagnostic: General 421
Table 174 Diagnostic: DSL Line 422
Table 175 Hardware Specifications 433
Table 176 Firmware Specifications 433
Table 177 Voice Features 438
Table 178 Wireless Features 440
Table 179 IEEE 802.11g 441
Table 180 Standards Supported 441
Table 181 P-2602HWL Series Power Adaptor Specifications 442
Table 182 Subnet Masks 478
Table 183 Subnet Masks 479
Table 184 Maximum Host Numbers 479
Table 185 Alternative Subnet Mask Notation 479
Table 186 Subnet 1 481
Table 187 Subnet 2 482
Table 188 Subnet 3 482
Table 189 Subnet 4 482
Table 190 Eight Subnets 482
Table 191 24-bit Network Number Subnet Planning 483
Table 192 16-bit Network Number Subnet Planning 483
Table 193 IEEE 802.11g 489
Table 194 Wireless Security Levels 490
Table 195 Comparison of EAP Authentication Types 493
Table 196 Wireless Security Relational Matrix 496
Table 197 Examples of Services 499
Table 198 Abbreviations Used in the Example Internal SPTGEN Screens Table 505
Table 199 Menu 1 General Setup 506
Table 200 Menu 3 506
Table 201 Menu 4 Internet Access Setup 509
Table 202 Menu 12 511
Table 203 Menu 15 SUA Server Setup 515
Table 204 Menu 21.1 Filter Set #1 517
Table 205 Menu 21.1 Filer Set #2, ... 520
Table 206 Menu 23 System Menus 524
Table 207 Menu 24.11 Remote Management Control 526
Table 208 Command Examples 526

PART I
Introduction

Introducing the ZyXEL Device (43)
Tutorial (51)
Introducing the Web Configurator (81)

1

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The P-2602HWUDL-D series are Integrated Access Devices (IADs) that combine an ADSL2+ router with Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog telephone to make Internet calls. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The P-2602HWUDL-D is also a complete security solution with a robust firewall and content filtering.

At the time of writing, this guide covers the following models.

Table 1 Models Covered

P-2602HWUDL-D1
P-2602HWUDL-D3

Please refer to the following description of the product name format.

- "H" denotes an integrated 4-port hub (switch). The "H" models also include Virtual Private Network (VPN) capability.
- "W" denotes wireless functionality. There is an embedded mini-PCI module for IEEE 802.11g wireless LAN connectivity. All wireless features documented in this user's guide refer to the "W" models only.
- "U" denotes USB port(s) used to share files via a USB memory stick or a USB hard drive. The ZyXEL Device can also function as a print server with an USB printer connected.
- "D" denotes a built-in DECT (Digital Enhanced Cordless Telecommunications) base station. Any DECT GAP phone can register with the ZyXEL Device to make calls to other registered DECT phones, make VoIP calls or make calls via the PSTN line.
- "L" denotes the PSTN (Public Switched Telephone Network) line feature. The PSTN line lets you have VoIP phone service and PSTN phone service at the same time. All PSTN line features documented in this user's guide refer to the "L" models only.

When the ZyXEL Device does not have power, the phone(s) connected to the **PHONE** port can still be used for making PSTN calls. Only one phone can be in use at a time.

- Models ending in “1”, for example P-2602HWUDL-D1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

Only use firmware for your ZyXEL Device’s specific model. Refer to the label on the bottom of your ZyXEL Device.

All screens displayed in this user’s guide are from the P-2602HWUDL-D1 model.

See the appendix on product specifications for a full list of features.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User’s Guide.
- SPTGEN. SPTGEN is a text configuration file that allows you to configure the device by uploading an SPTGEN file. This is especially convenient if you need to configure many devices of the same type.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

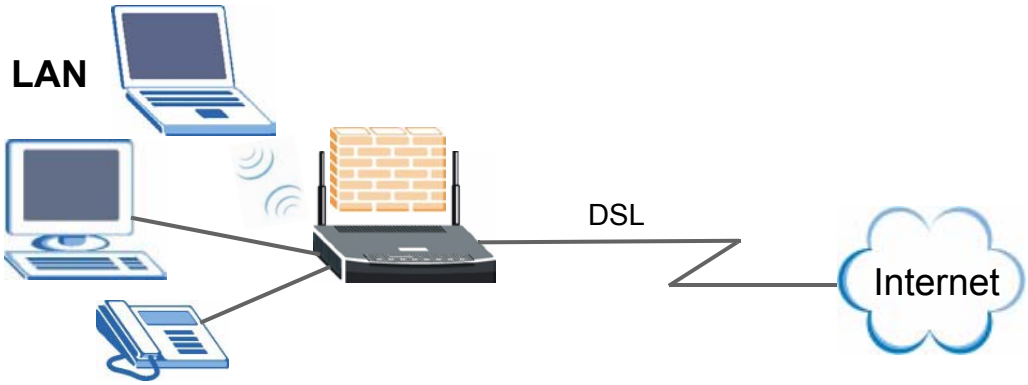
1.4 Applications for the ZyXEL Device

Here are some example uses for which the ZyXEL Device is well suited.

1.4.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the ZyXEL Device's LAN ports (or wirelessly).

Figure 1 ZyXEL Device's Router Features



You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

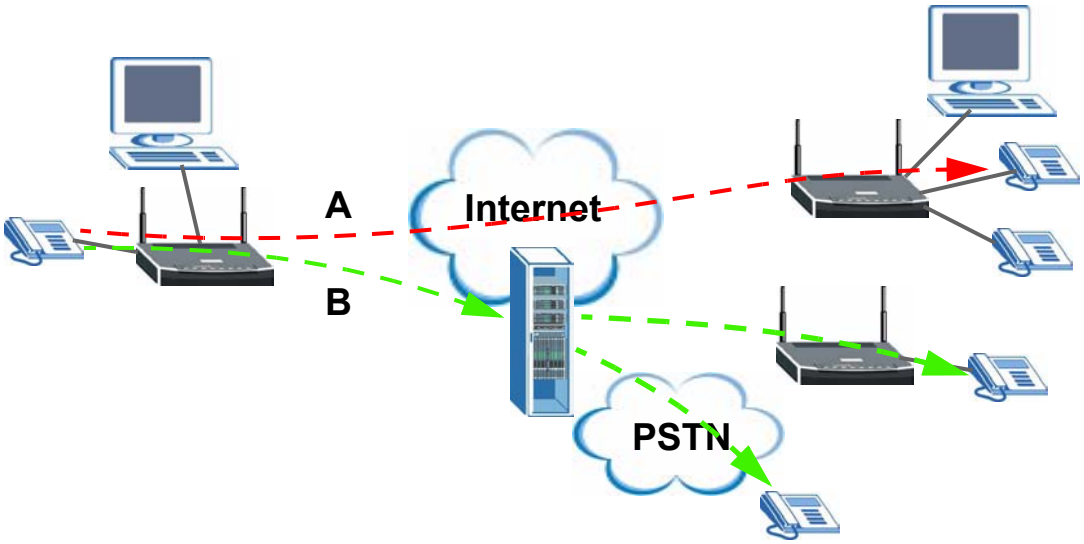
Use content filtering to block access to specific web sites, with URL's containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

Use bandwidth management to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.4.2 VoIP Features

You can register up to 10 SIP (Session Initiation Protocol) accounts and use the ZyXEL Device to make and receive VoIP telephone calls:

Figure 2 ZyXEL Device's VoIP Features

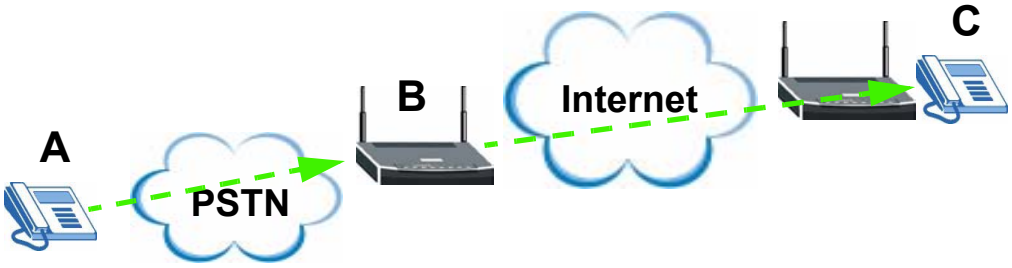


- Peer-to-Peer calls (**A**) - Use the ZyXEL Device to make a call to the recipient's IP address without using a SIP proxy server.
- Calls via a VoIP service provider (**B**) - The ZyXEL Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.4.3 VoIP Trunking Gateway

VoIP trunking allows you to use your ZyXEL Device as a gateway between VoIP and PSTN networks.

Figure 3 ZyXEL Device as a VoIP Trunking Gateway

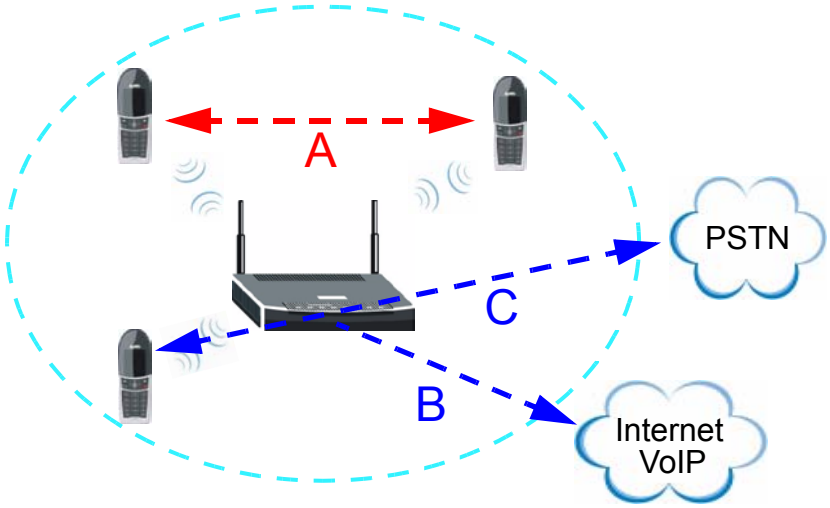


In this example, you use your analog phone (**A**) to call the ZyXEL Device (**B**). The ZyXEL Device changes the call into VoIP and sends it via the Internet to another VoIP phone (**C**).

1.4.4 DECT Base Station Feature

Your ZyXEL Device has a built in Digital Enhanced Cordless Telecommunications (DECT) base station. DECT is an ETSI (European Telecommunications Standards Institute) standard for digital cordless phones which specifies how they transmit, receive and process data and voice communication. You can register any DECT GAP phone with the ZyXEL Device.

Figure 4 DECT Base Station Feature



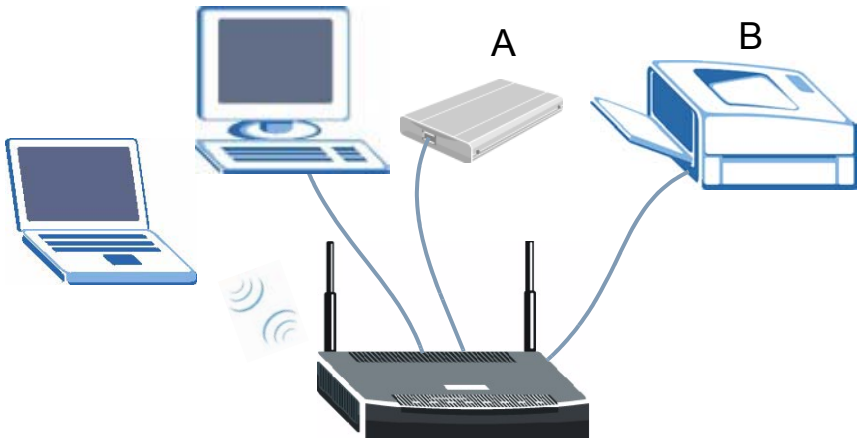
You can use your DECT phone to make calls to other DECT phones (**A**) registered with the ZyXEL Device. These calls are referred to as internal calls.

You can also use your DECT phone to make VoIP calls (**B**). For the PSTN models, you can also make calls via the PSTN line (**C**). These types of calls are referred to as external calls.

1.4.5 ZyXEL Device's USB Support

Use the built-in USB 2.0 ports to share files via a USB memory stick or a USB hard drive (**A**). You can also add a printer (**B**) and make it available on your local area network.

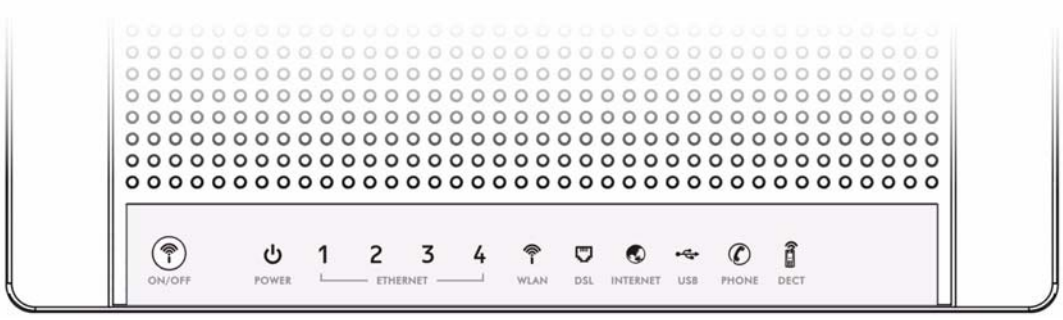
Figure 5 File Sharing Overview



1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 6 LEDs on the Top of the Device



None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
		Blinking	The ZyXEL Device is self-testing.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is not receiving power.
ETHERNET 1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is sending/receiving data to /from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WLAN	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g mode.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
		OFF	The wireless network is not activated.
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
USB	Green	On	The ZyXEL Device recognizes a USB connection.
		Blinking	The ZyXEL Device is sending/receiving data to /from the USB device connected to it.
		Off	The ZyXEL Device does not detect a USB connection.
PHONE	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
		Off	The phone port does not have a SIP account registered.
DECT	Orange	On	One of the DECT phone's associated SIP accounts for outgoing calls is registered and there is a voice message for the associated SIP account.
		Blinking (slow)	One of the DECT phones has its receiver off of the hook and there is a voice message for the associated SIP account.
		Blinking (Fast)	The DECT base station is in registration mode. DECT phones can register with the DECT base station. One of the DECT phones is logging on if the green LED is blinking at the same time.
	Green	On	One of the DECT phone's associated SIP accounts for outgoing calls is registered.
		Blinking (slow)	One of the DECT phones has its receiver off of the hook.
		Blinking (Fast)	One of the DECT phones is logging on if the orange LED is blinking at the same time.
		Off	The DECT base station is not in registration mode and there is not a registered SIP account associated with any of the DECT phones.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234". You can also use the

1.6.1 Using the Reset Button

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.7 The WLAN Button

You can use the **ON/OFF** WLAN button ( ) on the top of the device to turn the wireless LAN off or on. You can also use it to activate OTIST in order to assign your ZyXEL Device's wireless security settings to wireless clients.

1.7.1 Turn the Wireless LAN Off or On

1 Make sure the **POWER** LED is on (not blinking).
2 Press the WLAN button for one second and release it. The **WLAN** LED should change from on to off or vice versa.

1.7.2 Activate OTIST

1 Make sure the **POWER** LED is on (not blinking).
2 Press the WLAN button for five seconds and release it. The **WLAN** LED should flash while the device uses OTIST to send wireless settings to OTIST clients.

You must activate OTIST in the ZyXEL Device and in the wireless device(s) within three minutes of each other. See Section 10.6 on page 165 for more information.

2

Tutorial

This chapter describes how to

2.1 How to Set up a Wireless Network

This section gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

2.2 Example Parameters

SSID	SSID_Example3
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	Mixed (IEEE 802.11b/g)

An access point (AP) or wireless router is referred to as “AP” and a computer with a wireless network card or USB/PCI adapter is referred to as “wireless client” here.

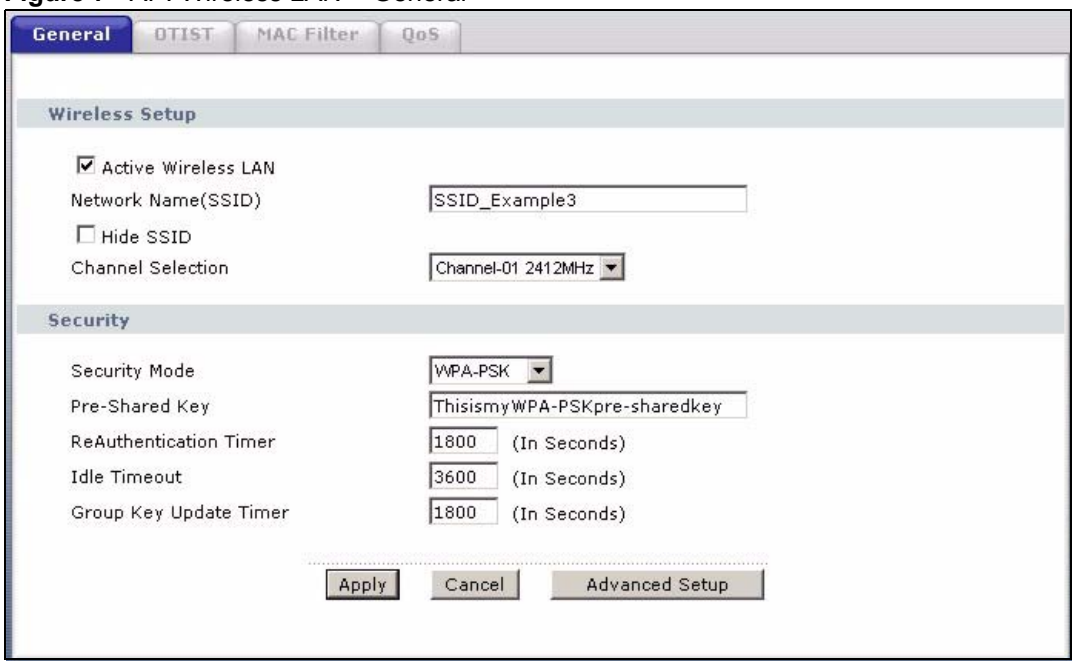
We use the P-2602HWUDL-D1 web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

2.3 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

1 Open the **Network > Wireless LAN > General** screen in the AP’s web configurator.

Figure 7 AP: Wireless LAN > General



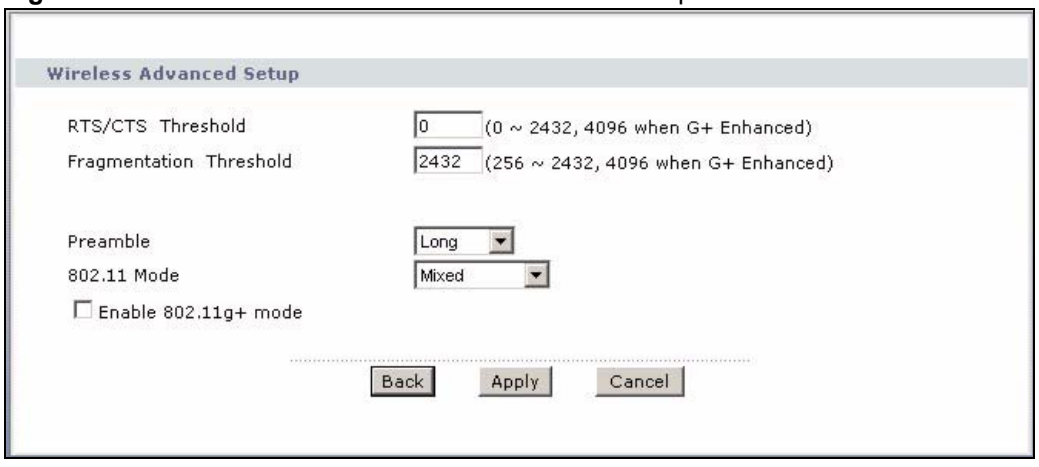
2 Make sure the **Active Wireless LAN** check box is selected.

3 Enter "SSID_Example3" as the SSID and select a channel which is not used by another AP.

4 Set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.

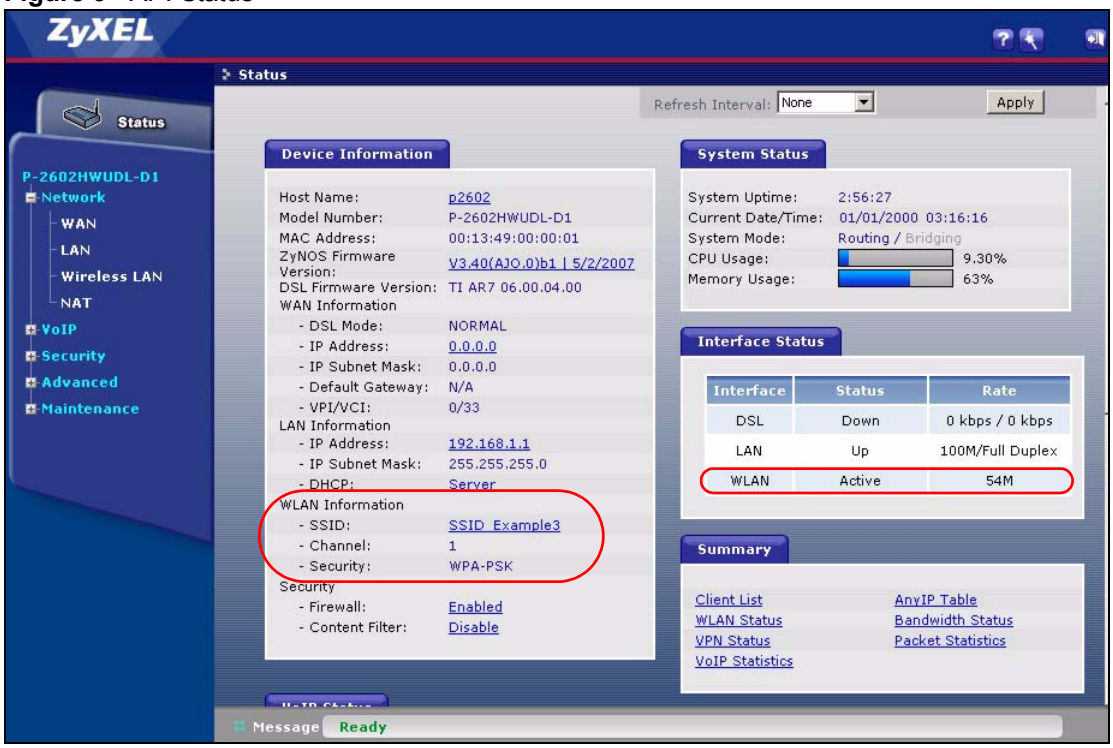
5 Click the **Advanced Setup** button and select **Mixed** in the **802.11 Mode** field. Click **Apply**.

Figure 8 AP: Wireless LAN > General > Advanced Setup



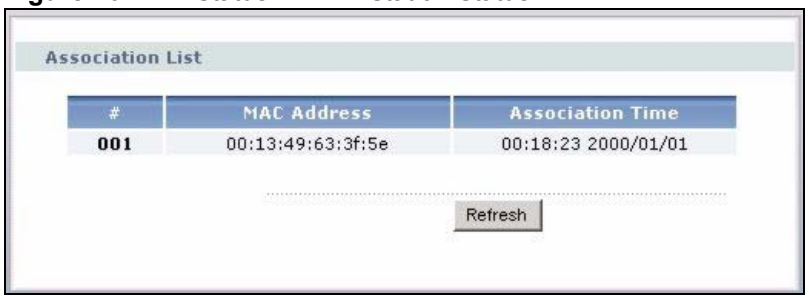
6 Open the **Status** screen.Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 9 AP: Status



7 Click the **WLAN Station Status** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 10 AP: Status: WLAN Station Status

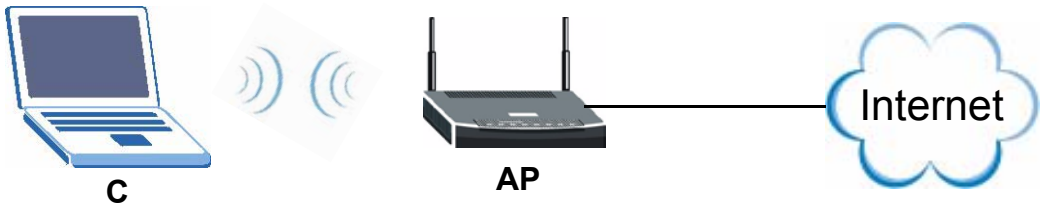


2.4 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

2.4.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



There are three ways to connect the client to an access point.

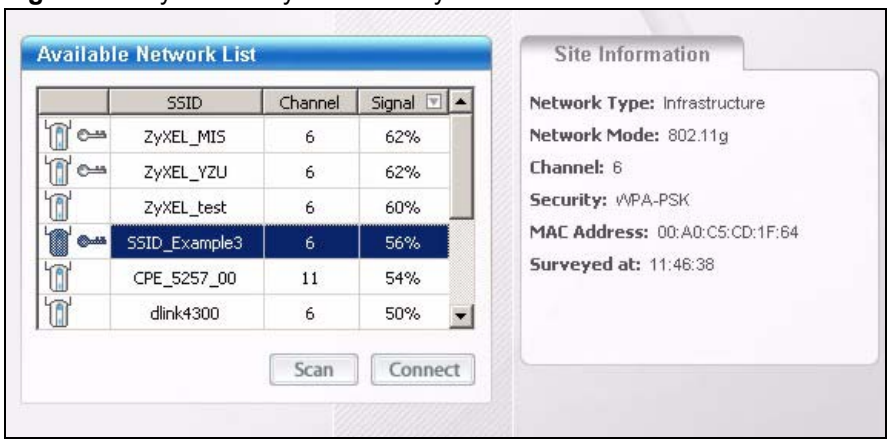
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is "SSID_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 11 ZyXEL Utility: Site Survey

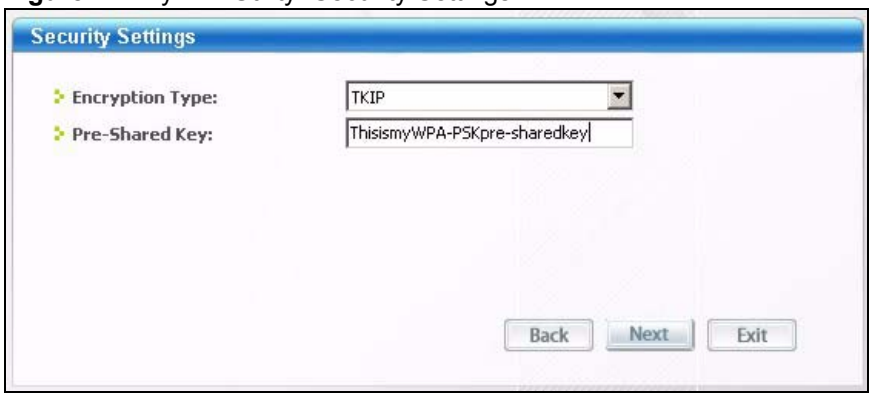


2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

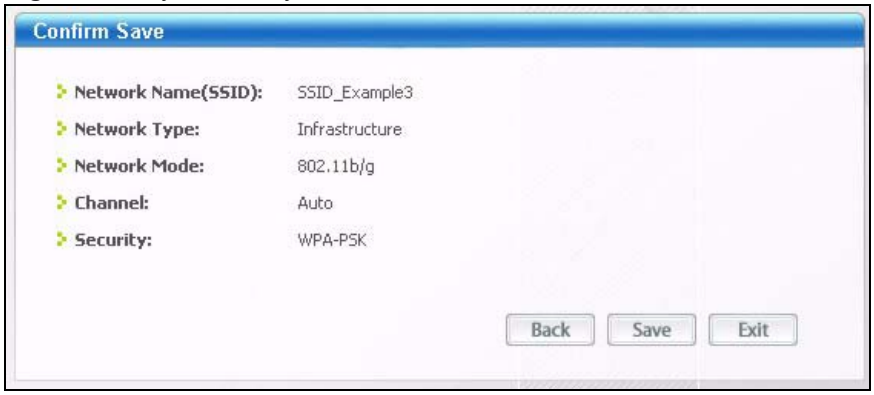
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 12 ZyXEL Utility: Security Settings



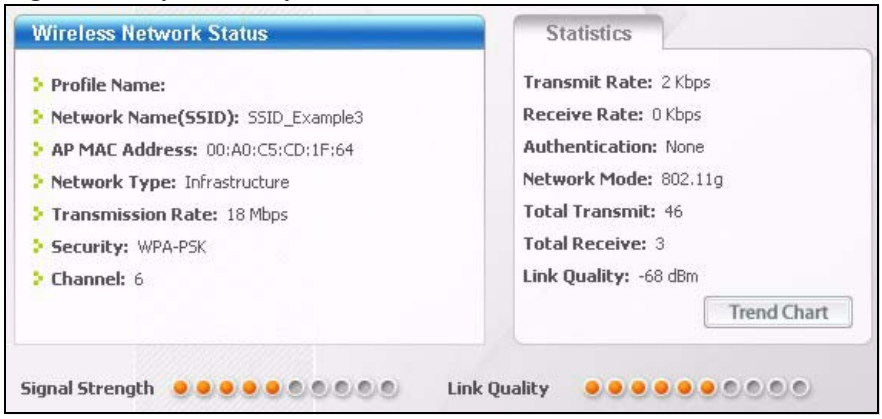
4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 13 ZyXEL Utility: Confirm Save



5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 14 ZyXEL Utility: Link Info



6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

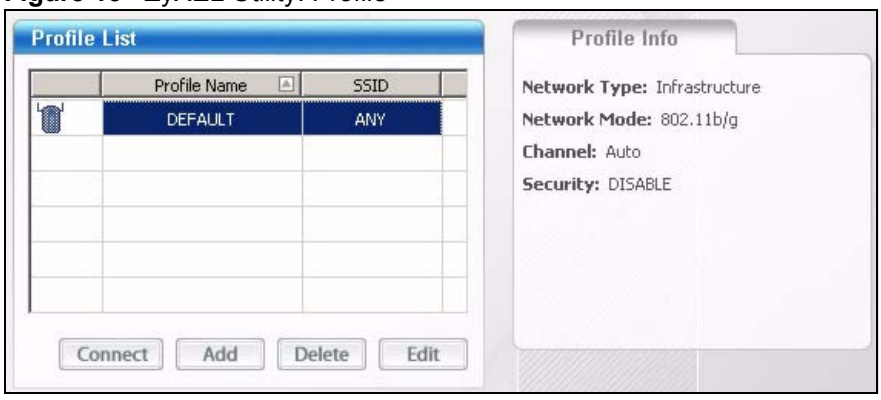
2.4.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is "SSID_Example3", the profile name is "PN_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

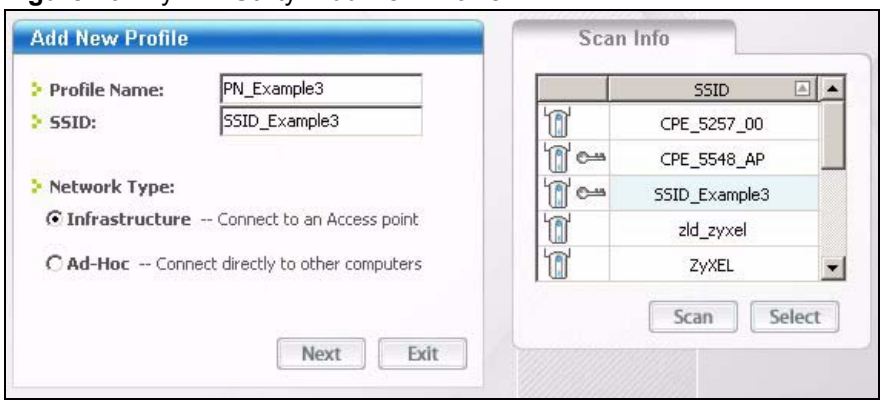
1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 15 ZyXEL Utility: Profile



2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

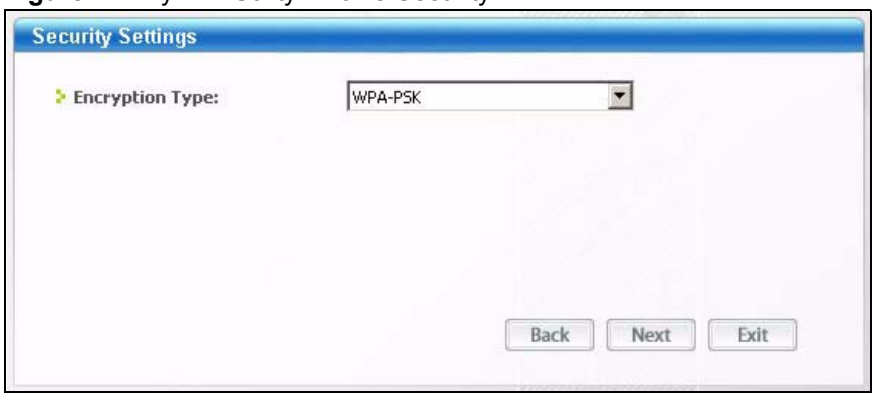
Figure 16 ZyXEL Utility: Add New Profile



3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

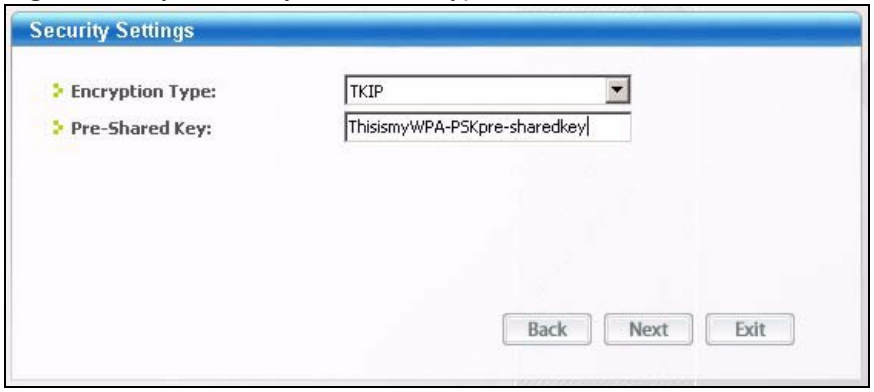
4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 17 ZyXEL Utility: Profile Security



5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Figure 18 ZyXEL Utility: Profile Encryption

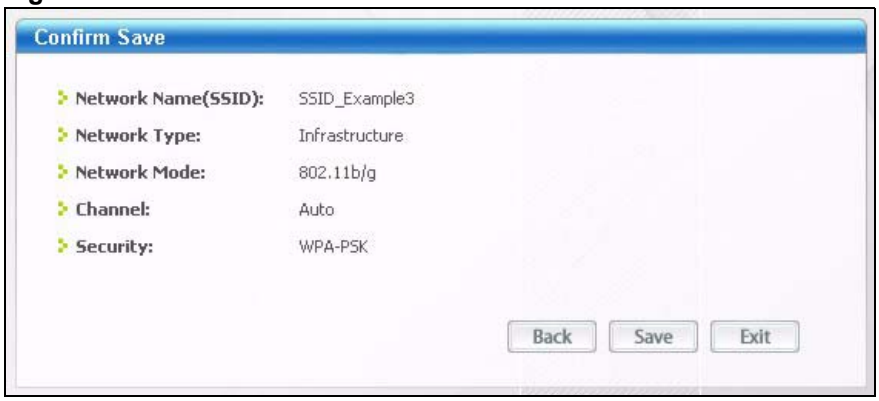


6 In the next screen, leave both boxes checked.

Figure 19 Profile: Wireless Protocol Settings.

7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

Figure 20 Profile: Confirm Save



8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Only one profile can be activated and used at any given time.

Figure 21 Profile: Activate

9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

10 Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

2.5 Using NAT with Multiple Public IP Addresses

This chapter shows you examples of how to set up your ZyXEL Device if you have more than one fixed (static) IP address from your ISP.

2.5.1 Example Parameters and Scenario

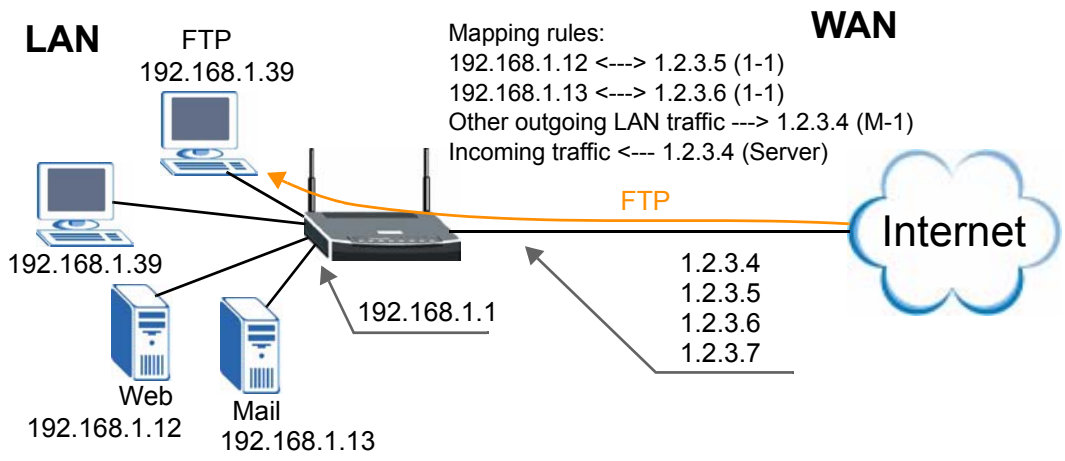
The following table shows the public IP addresses from your ISP and your ZyXEL Device's LAN IP address.

Public IP Addresses	1.2.3.4 to 1.2.3.7
ZyXEL Device's LAN IP Address	192.168.1.1

The following figure shows the network you want to set up in this example.

- Assign the first public address (1.2.3.4) to the ZyXEL Device's WAN port.
- Map the second and third public IP addresses (1.2.3.5 and 1.2.3.6) to the web and mail servers (192.168.1.12 and 192.168.1.13) respectively for traffic in both directions.
- Map the first public address (1.2.3.4) to outgoing traffic from other local computers.
- Map the first public address (1.2.3.4) to incoming traffic from the WAN.
- Forward FTP traffic using port 21 from the WAN to a specific local computer (192.168.1.39).
- The last public IP address (1.2.3.7) is not mapped to any device and is reserved for future use.

Figure 22 Tutorial Example: Using NAT with Static Public IP Addresses



To set up this network, we are going to:

1. Configure the WAN connection to use the first public IP address (1.2.3.4).
2. Configure NAT address mapping for other public IP addresses (1.2.3.5 and 1.2.3.6).
3. Configure NAT port forwarding to forward FTP traffic from the WAN to a specific computer on your local network.

2.5.2 Configuring the WAN Connection with a Static IP Address

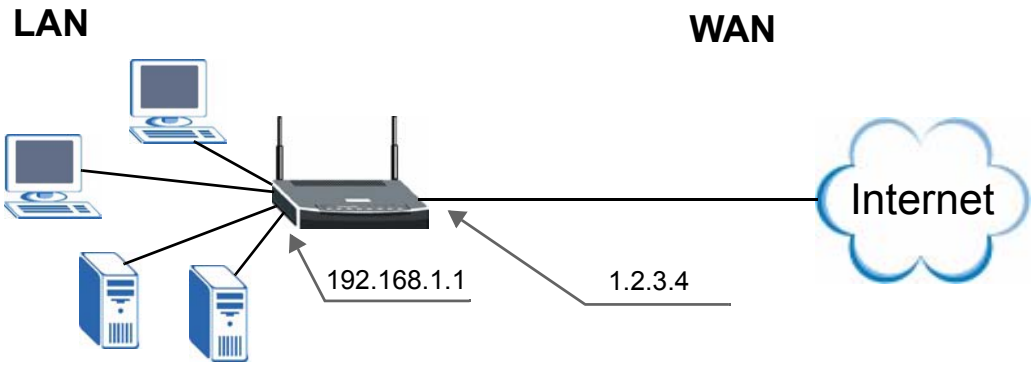
The following table shows the information your ISP gave you for Internet connection.

Encapsulation	PPPoE
VPI/VCI	8/33

Public IP Addresses	1.2.3.4 1.2.3.5 1.2.3.6 1.2.3.7
Gateway IP Address	1.2.3.89
Subnet Mask	255.255.255.0
User Name	exampleuser
Password	abcd1234
DNS Server	1.2.1.1 1.2.1.2

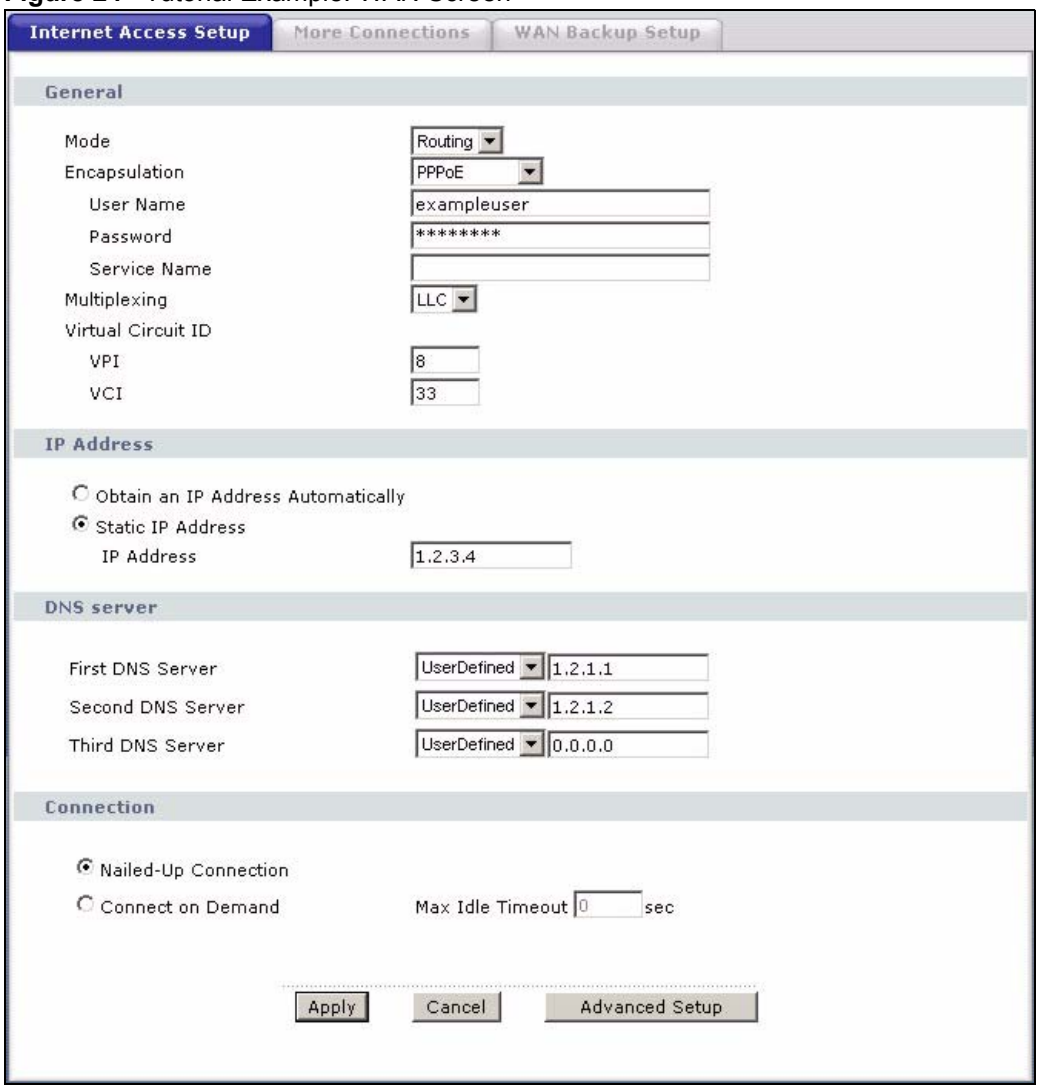
Follow the steps below to configure your ZyXEL Device for Internet access using PPPoE in this example.

Figure 23 Tutorial Example: WAN Connection with a Static Public IP Address



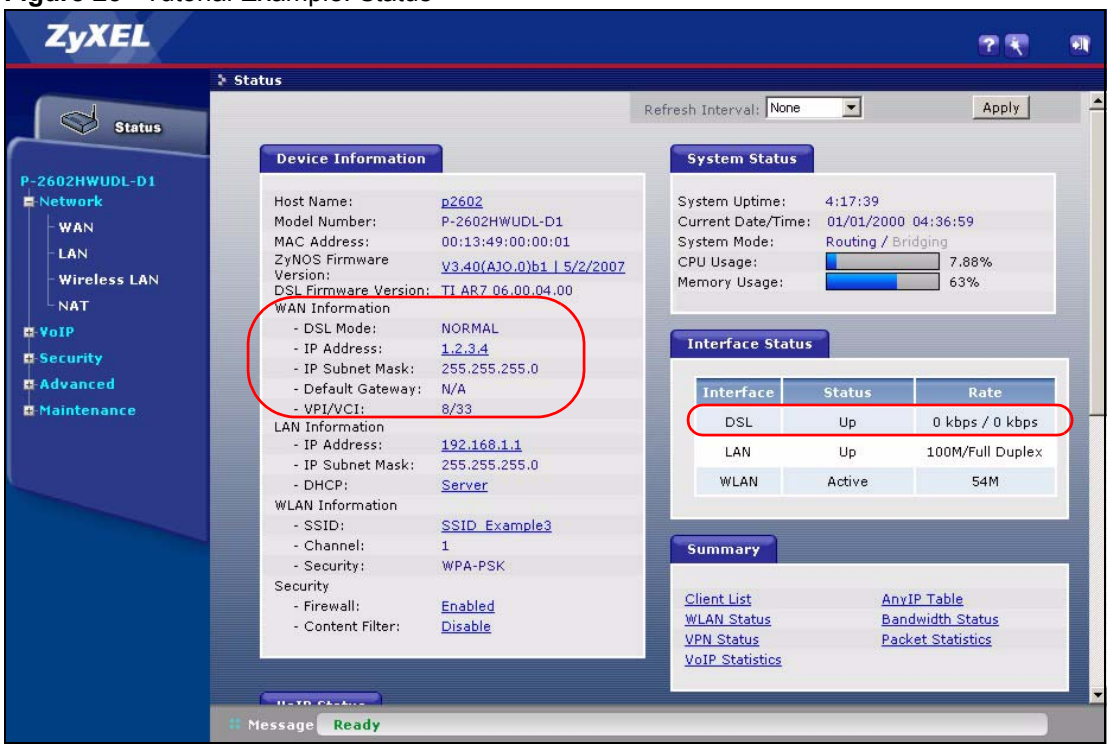
1. Click **Network** > **WAN**.
2. Select **Routing** in the **Mode** field and select **PPPoE** from the **Encapsulation** drop-down list box.
3. Enter the information (such as the user name, password and VPI/VCI value) provided by your ISP. If your ISP didn't give you the service name, leave the field blank.
4. In the **IP Address** section, select **Static IP Address** and enter the first fixed public IP address ("1.2.3.4" in this example).
5. Configure the IP address of the DNS server the ZyXEL Device can query to resolve domain names. Select **UserDefined** and enter the first and second DNS server's IP addresses given by your ISP.
6. Click **Apply** to save your changes.

Figure 24 Tutorial Example: WAN Screen



7 Go to the **Home** screen to check your WAN connection status. Make sure the status is not down.

Figure 25 Tutorial Example: Status



2.5.3 Public IP Address Mapping

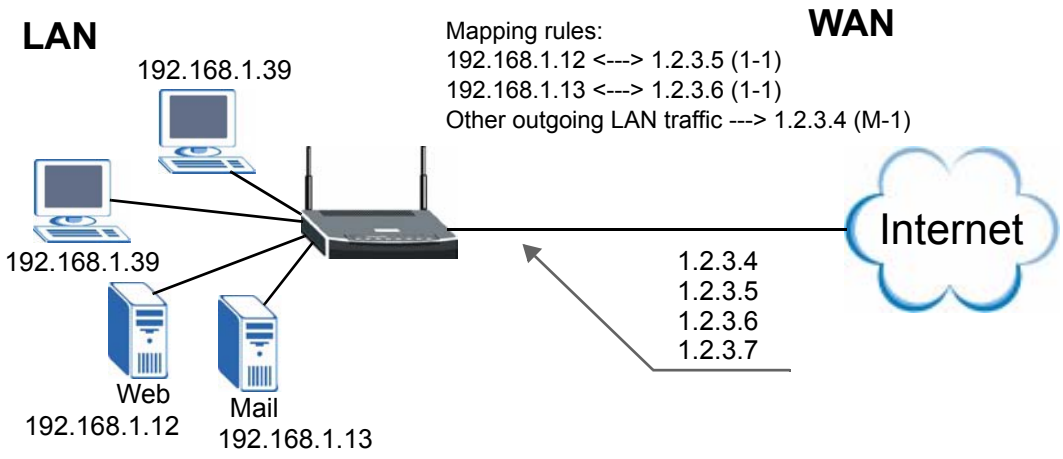
To have the local computers and servers use specific WAN IP addresses, you need to map static public IP addresses to them.

The one-to-one NAT address mapping rules are for both incoming and outgoing connections. The ZyXEL Device forwards traffic that is initiated from either the LAN or the WAN to the destination IP address.

The many-to-one or many-to-many NAT address mapping rules are for outgoing connections only. That means only traffic initiated from the LAN or returned packets are allowed to go through the ZyXEL Device.

In this example, you create two one-to-one rules to map the internal web server (192.168.1.12) and mail server (192.168.1.13) to different static public IP addresses. The many-to-one rule maps a public IP address (1.2.3.4, that is, the ZyXEL Device's WAN IP address) to outgoing LAN traffic. It allows other local computers on the same subnet as the ZyXEL Device's LAN IP address to use this IP address to access the Internet.

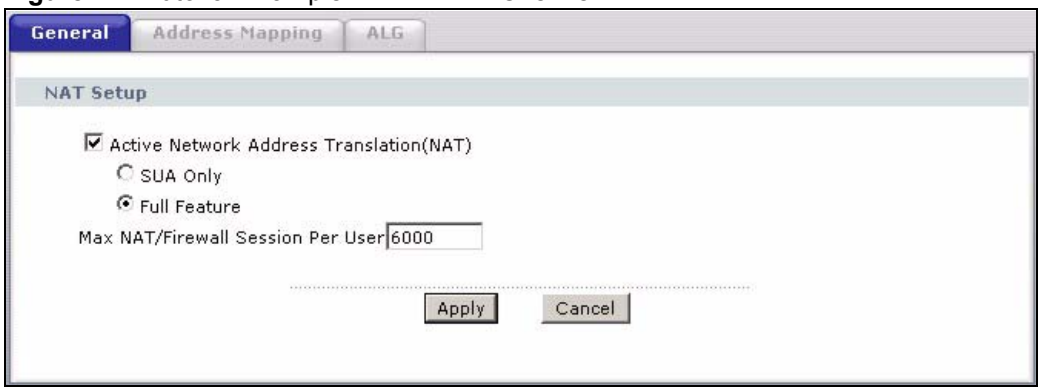
Figure 26 Tutorial Example: Mapping Multiple Public IP Addresses to Inside Servers



The ZyXEL Device applies the rules in the order that you specify. You should put any one-to-one rules before a many-to-one rule.

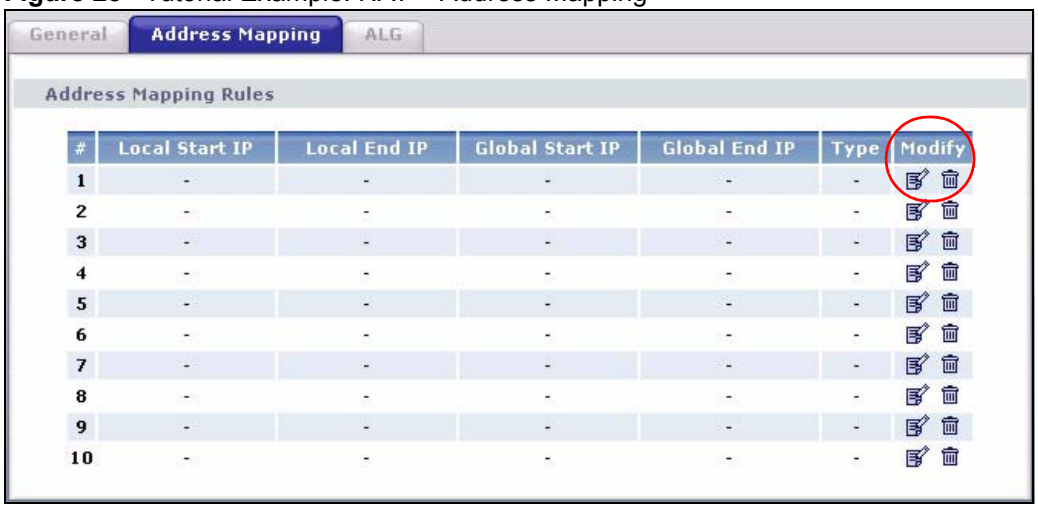
1 Click **Advanced** > **NAT**.
2 Enable NAT and select **Full Feature** as you have multiple public IP addresses to map to private IP addresses. Click **Apply**.

Figure 27 Tutorial Example: NAT > NAT Overview



3 Click the **Address Mapping** tab.
4 Click the first rule's **Edit** icon ( ) in the **Modify** column to display the **Address Mapping Rule** screen.

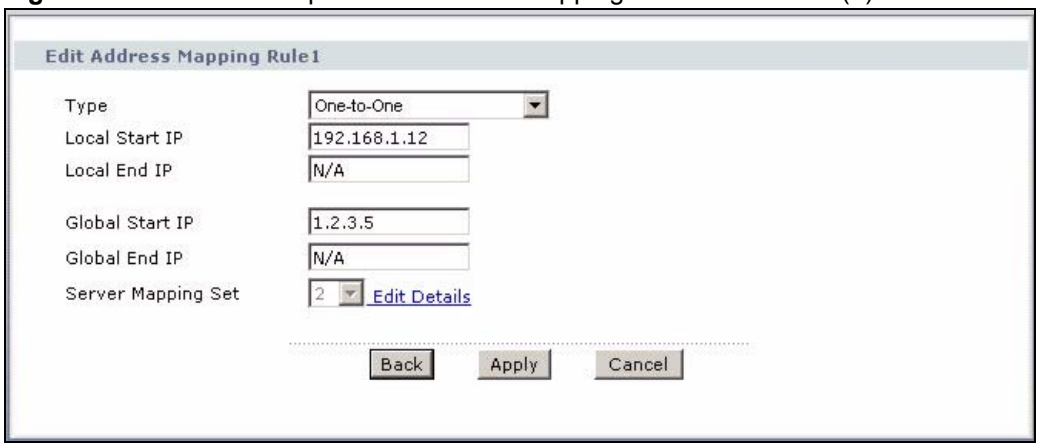
Figure 28 Tutorial Example: NAT > Address Mapping


General
Address Mapping
ALG
Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -
3 - - - - -
4 - - - - -
5 - - - - -
6 - - - - -
7 - - - - -
8 - - - - -
9 - - - - -
10 - - - - -

5 Map a public IP address to the web server.

Select the **One-to-One** type and enter 192.168.1.12 as the local start IP address and 1.2.3.5 as the global start IP address. Click **Apply**.

Figure 29 Tutorial Example: NAT Address Mapping Edit: One-to-One (1)

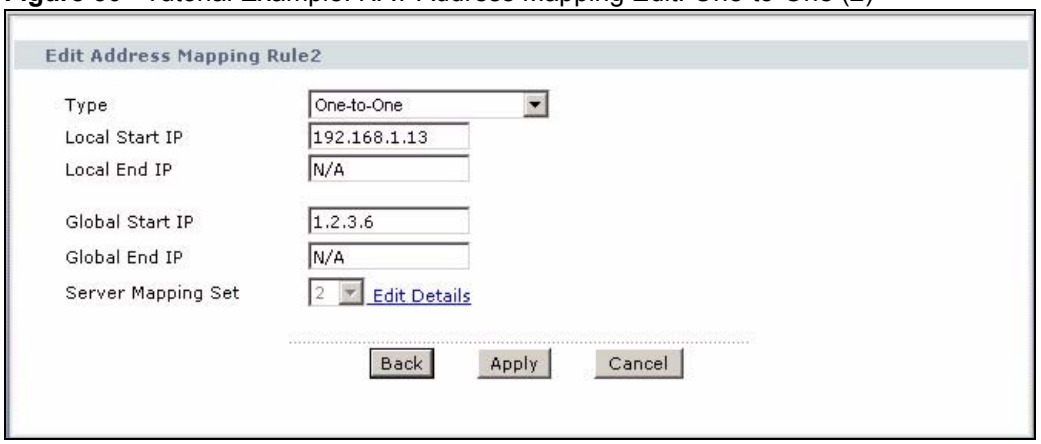


6 Click the second rule's **Edit** icon ( ).

7 Map a public IP address to the mail server.

Select the **One-to-One** type and enter 192.168.1.13 as the local start IP address and 1.2.3.6 as the global start IP address. Click **Apply**.

Figure 30 Tutorial Example: NAT Address Mapping Edit: One-to-One (2)

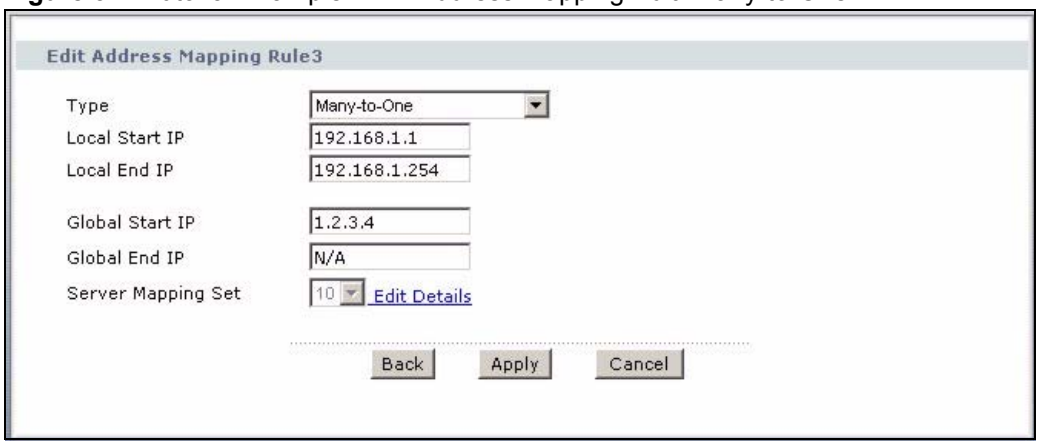


8 Click the third rule's **Edit** icon ( ).

9 Map a public IP address to other outgoing LAN traffic.

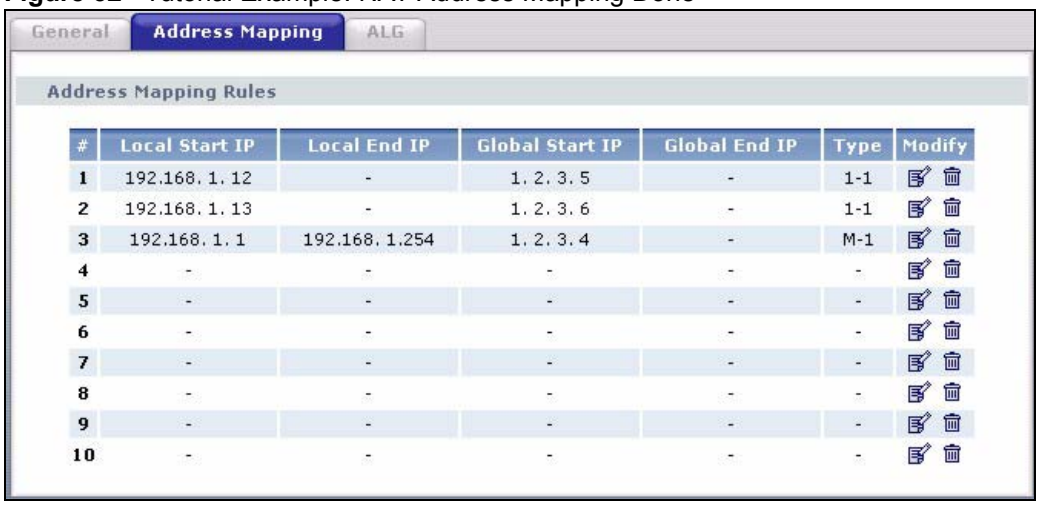
Select the **Many-to-One** type and enter 192.168.1.1 as the local start IP address, 192.168.1.254 as the local end IP address and 1.2.3.4 as the global start IP address. Click **Apply**.

Figure 31 Tutorial Example: NAT Address Mapping Edit: Many-to-One



10 After the configurations, the **Address Mapping** screen looks as shown. You still have one IP address (1.2.3.7) that can be assigned to another internal server when you expand your network.

Figure 32 Tutorial Example: NAT Address Mapping Done


General
Address Mapping
ALG
Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 192.168.1.12 - 1.2.3.5 - 1-1
2 192.168.1.13 - 1.2.3.6 - 1-1
3 192.168.1.1 192.168.1.254 1.2.3.4 - M-1
4 - - - - -
5 - - - - -
6 - - - - -
7 - - - - -
8 - - - - -
9 - - - - -
10 - - - - -

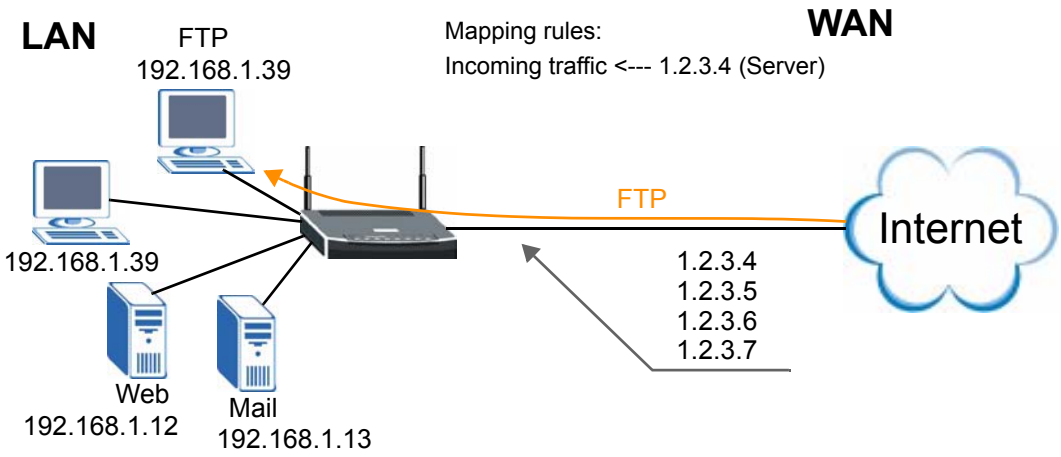
To allow traffic from the WAN to be forwarded through the ZyXEL Device, you must also create a firewall rule. Refer to Section 2.5.5 on page 67 for more information.

2.5.4 Forwarding Traffic from the WAN to a Local Computer

A server NAT address mapping rule allows computers behind the NAT be accessible to the outside world. To have the ZyXEL Device forward incoming traffic to a specific computer on your local network, you should also create a port forwarding (server mapping) rule.

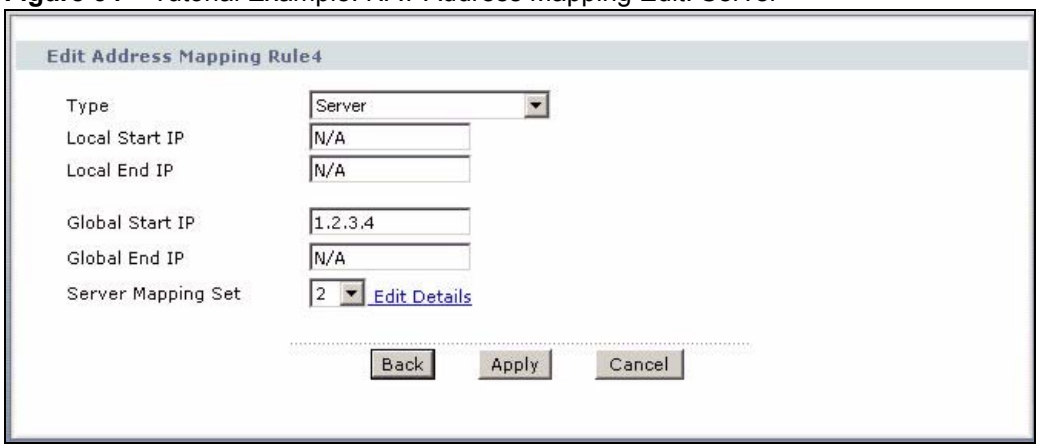
In this example, you want to forward FTP traffic using port 21 to the computer with the IP address of 192.168.1.39.

Figure 33 Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer



1 Click **Advanced** > **NAT** > **Address Mapping**.
2 Click the forth rule's **Edit** icon ( ) to configure a server rule.

Figure 34 Tutorial Example: NAT Address Mapping Edit: Server



3 Select a number and click the **Edit Details** link to edit a port forwarding set.

4 Select **FTP** from the **Service Name** drop-down list box, and enter "192.168.1.39" as the server IP address. Click **Add** to add the rule to the table.

5 Click **Apply** to go back to the **Edit Address Mapping Rule** screen. Click **Apply** again.

Figure 35 Tutorial Example: NAT Port Forwarding

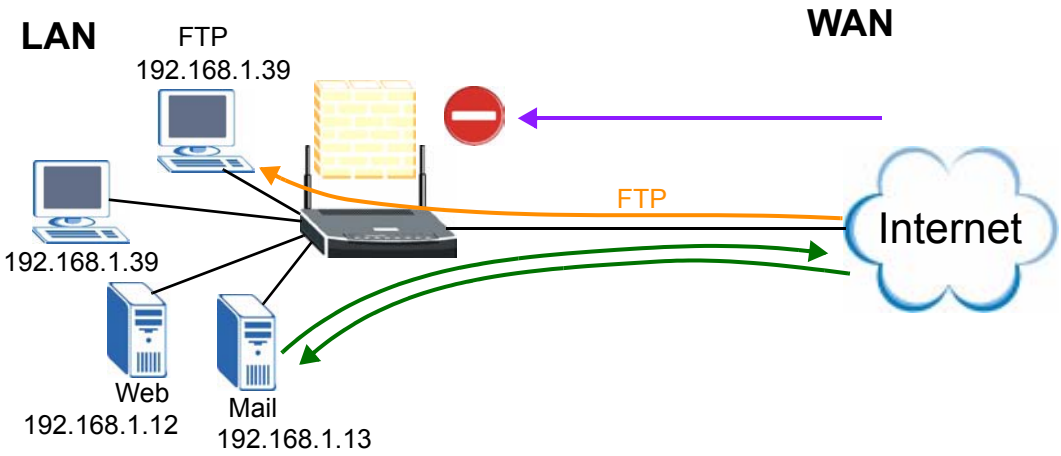
2.5.5 Allow WAN-to-LAN Traffic through the Firewall

By default, the ZyXEL Device blocks any traffic initiated from the WAN to the LAN. To have the ZyXEL Device forward traffic initiated from the WAN to a local computer or server on the LAN, you need to configure a firewall rule to allow it.

In this example, you create the firewall rules to allow traffic from the WAN to the following servers on the LAN:

- Web server
- Mail server
- FTP server

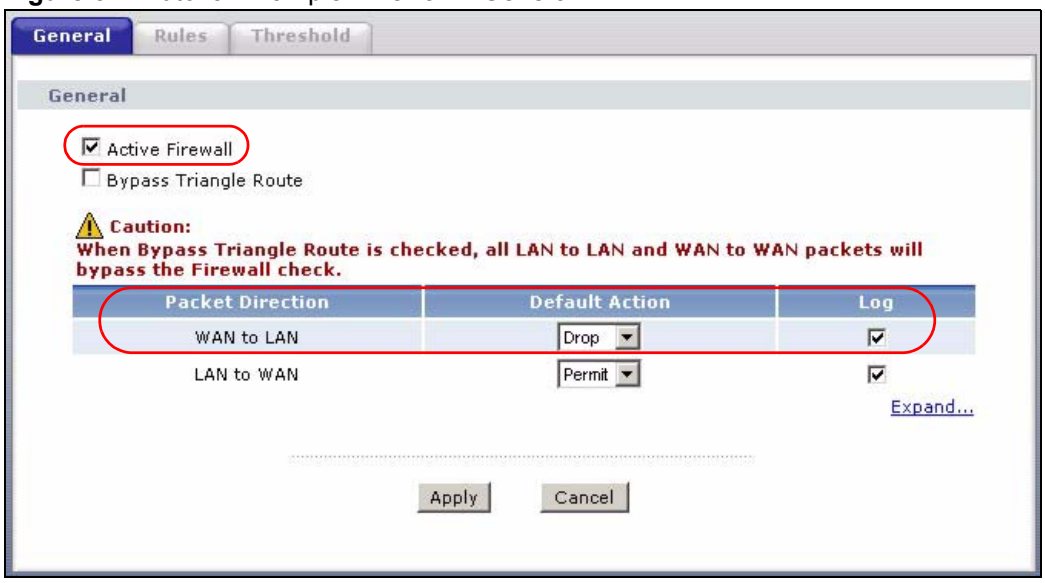
Figure 36 Tutorial Example: Allow WAN-to-LAN Traffic



1 Click **Security** > **Firewall**.

2 Make sure the firewall is enabled and traffic from the WAN to the LAN is dropped.

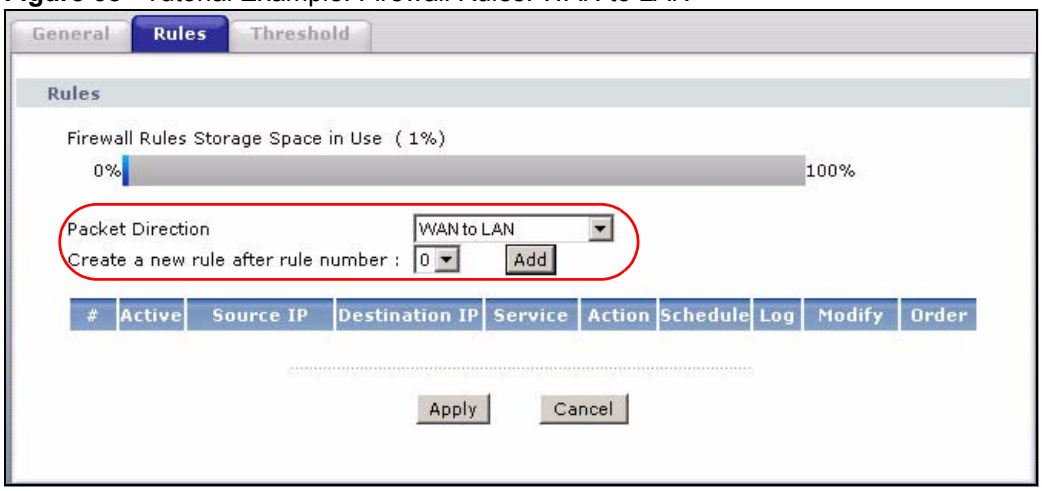
Figure 37 Tutorial Example: Firewall > General



3 Go to the **Rules** screen.

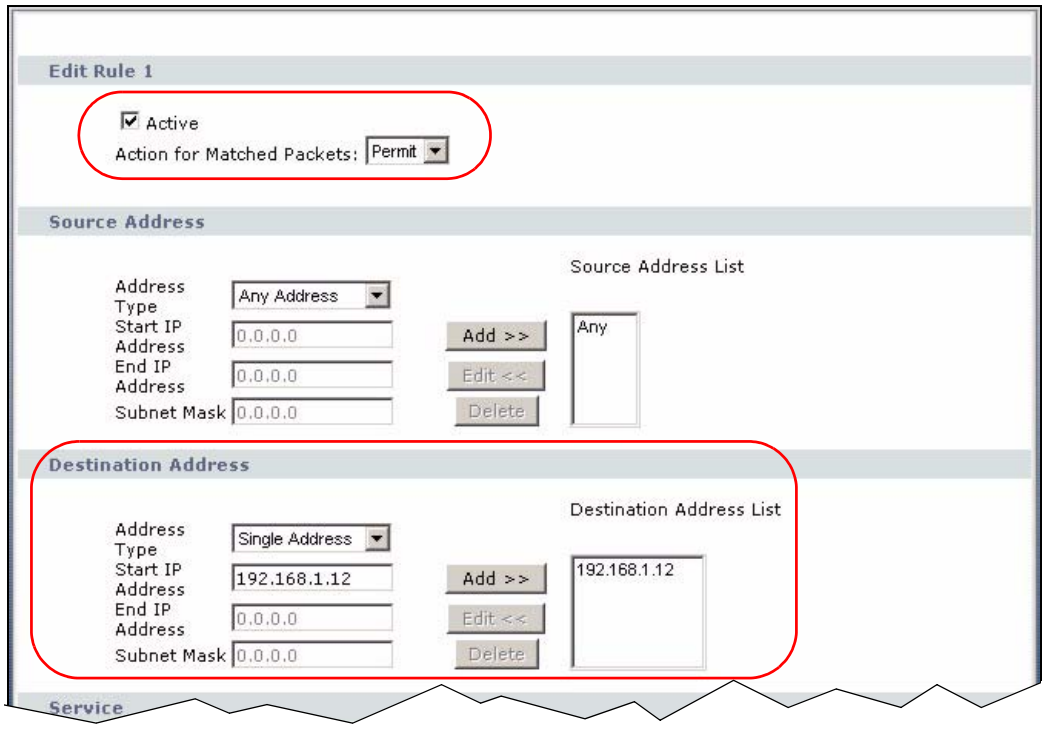
4 Select the **WAN to LAN** packet direction and click the **Add** button to create a new firewall rule.

Figure 38 Tutorial Example: Firewall Rules: WAN to LAN



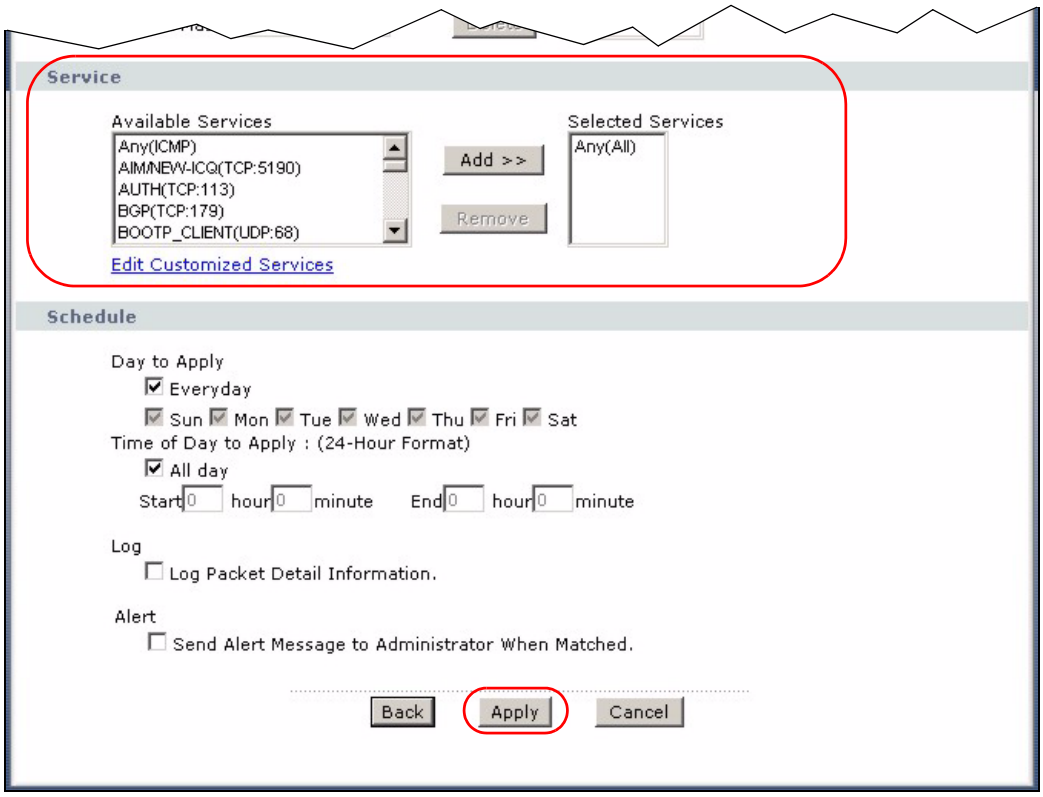
5 Configure a firewall rule to allow traffic from the WAN to the web server.
Select **Any** in the **Destination Address List** box and click **Delete**.
Select **Single Address** as the destination address type. Enter "192.168.1.12" and click **Add >>**.

Figure 39 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Web Server



6 Select **Any(All)** in the **Available Services** box on the left, and click **Add** >> to add it to the **Selected Services** box on the right. Click **Apply**.

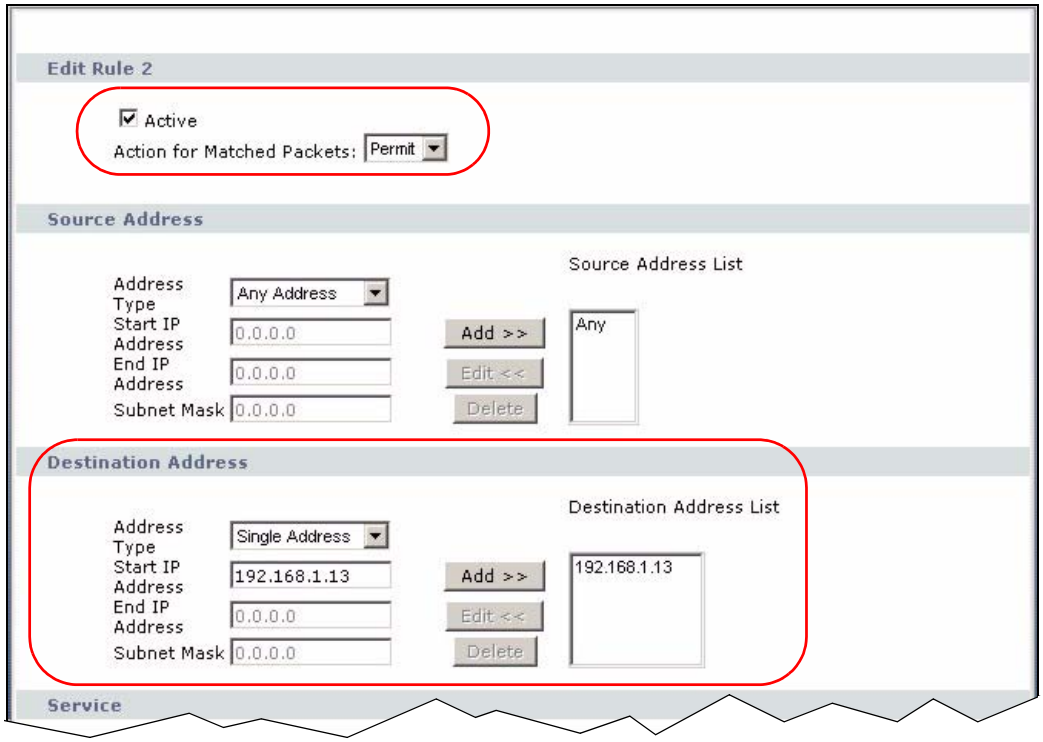
Figure 40 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Web Server



7 Click the **Add** button to configure a firewall rule to allow traffic from the WAN to the mail server.

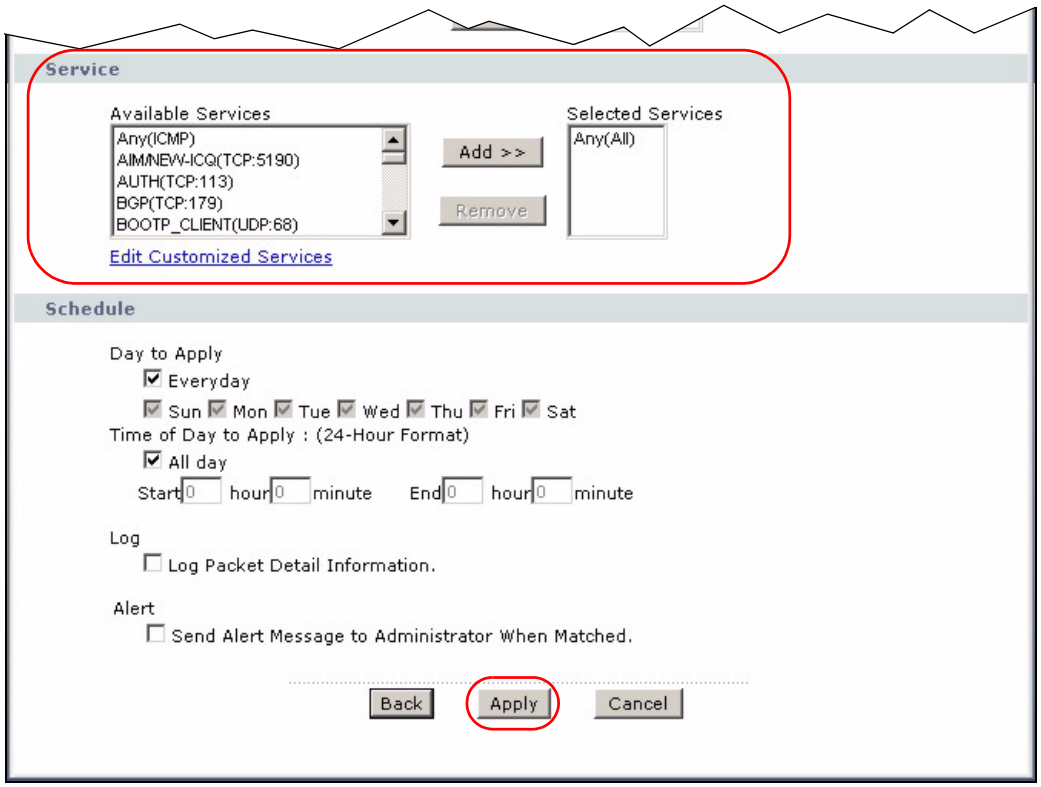
Select **Any** in the **Destination Address List** box and click **Delete**.
Select **Single Address** as the destination address type. Enter “192.168.1.13” and click **Add**.

Figure 41 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Mail Server



8 Select **Any(All)** in the **Available Services** box on the left, and click **Add >>** to add it to the **Selected Services** box on the right. Click **Apply**.

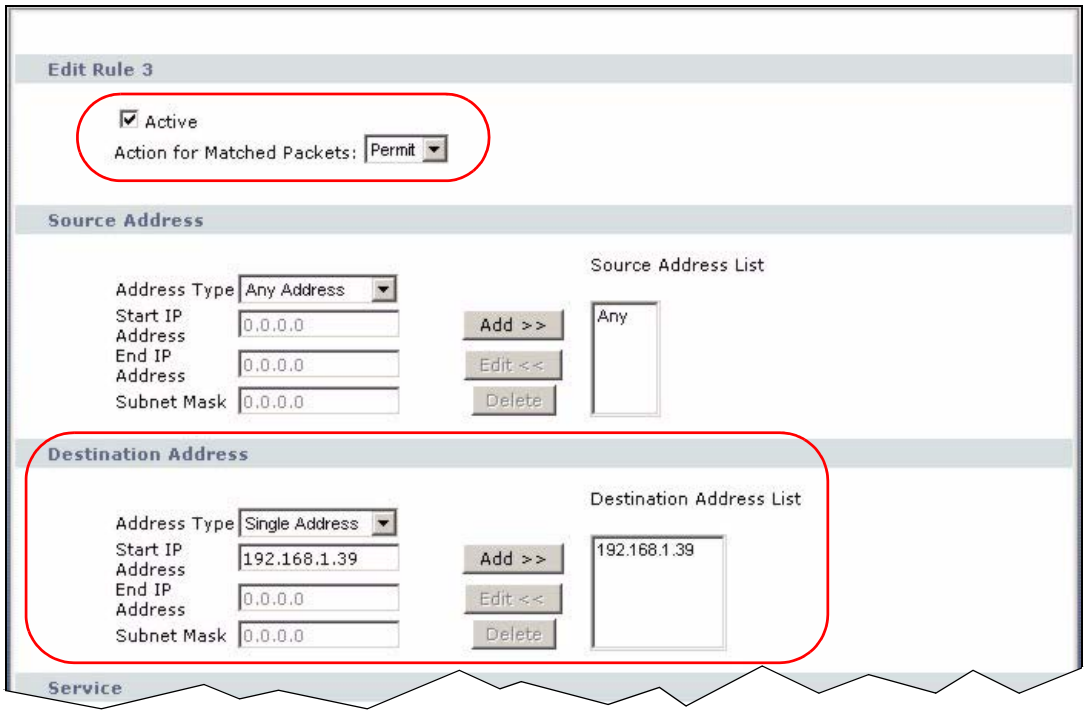
Figure 42 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Mail Server



9 Click the **Add** button to configure a firewall rule to allow FTP traffic from the WAN to the FTP server.

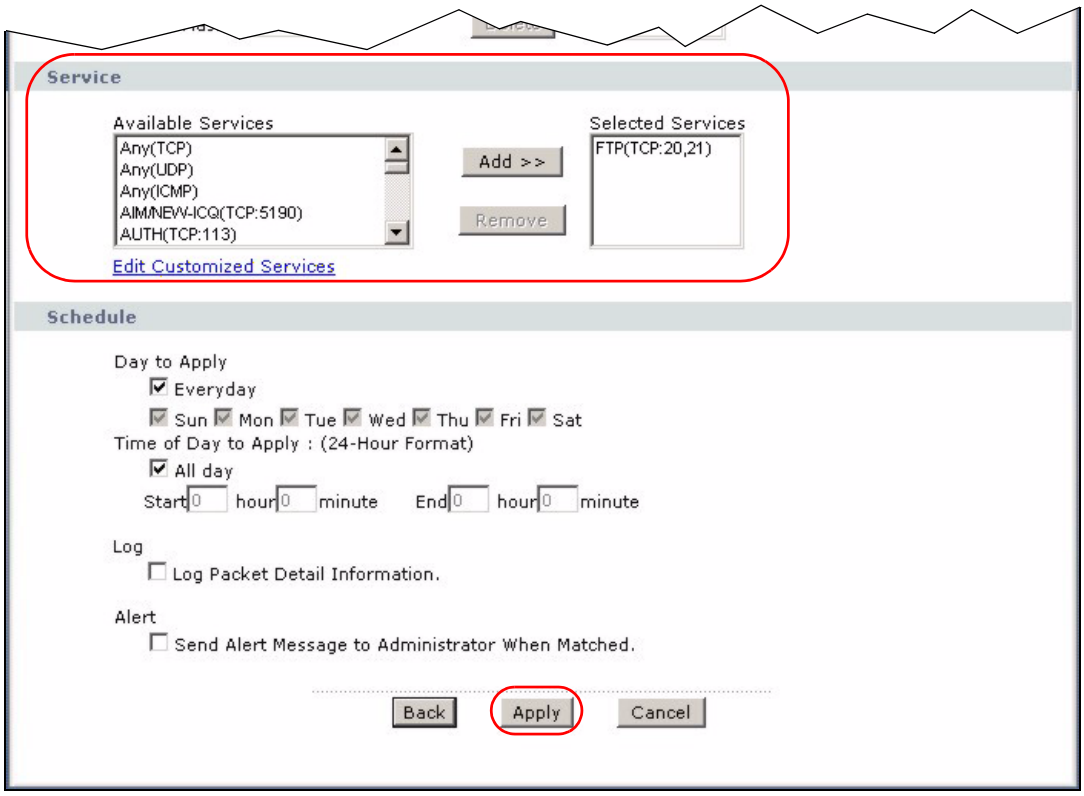
Select **Any** in the **Destination Address List** box and click **Delete**.
Select **Single Address** as the destination address type. Enter "192.168.1.39" and click **Add**.

Figure 43 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for FTP Server



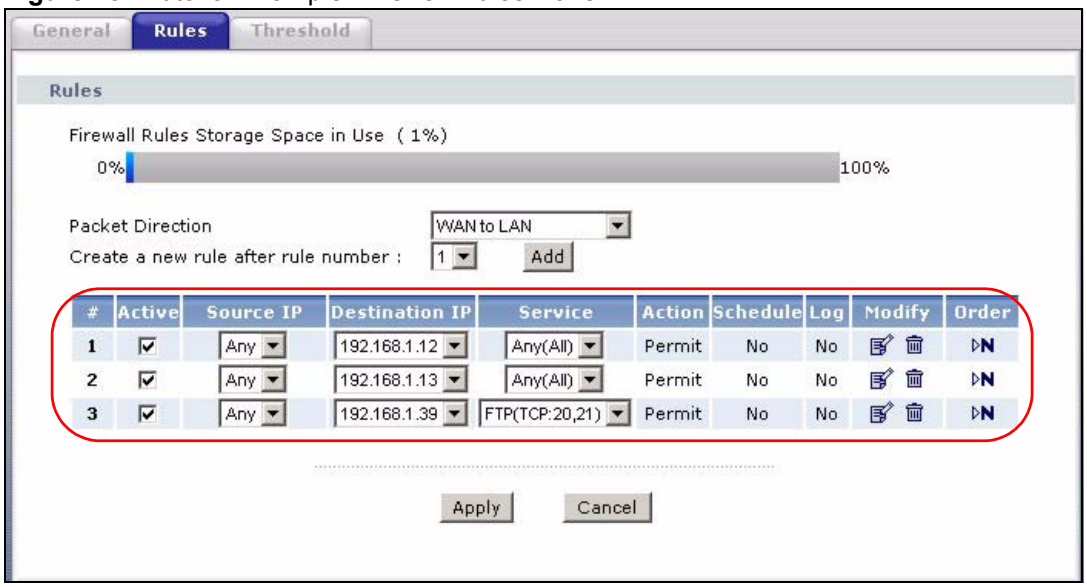
10 Select **FTP(TCP:20,21)** in the **Available Services** box on the left, and click **Add >>** to add it to the **Selected Services** box on the right. Click **Apply**.

Figure 44 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for FTP Server



11 When you are done, the **Rules** screen looks as shown.

Figure 45 Tutorial Example: Firewall Rules Done



2.5.6 Testing the Connections

1 Open the web browser on one of the local computers and enter any web site's URL in the address bar. If you can access the web site, your WAN connection and NAT address mapping are configured successfully. If you cannot access it, make sure you entered the

correct information in the **WAN** and **NAT Address Mapping** screens. Also check that the Internet account is active and the computer's IP address is in the same subnet as the ZyXEL Device.

2. Open your web browser and try accessing the web server (1.2.3.5) from the outside network. If you cannot access the web server, make sure the NAT address mapping rule is configured correctly and there is a firewall rule to allow HTTP traffic from the WAN to the web server.
3. Try accessing the FTP server (1.2.3.4) from the outside network to send or retrieve a file. If you cannot access the FTP server, make sure the NAT port forwarding rule is active and there is a firewall rule to allow FTP traffic from the WAN to FTP server.

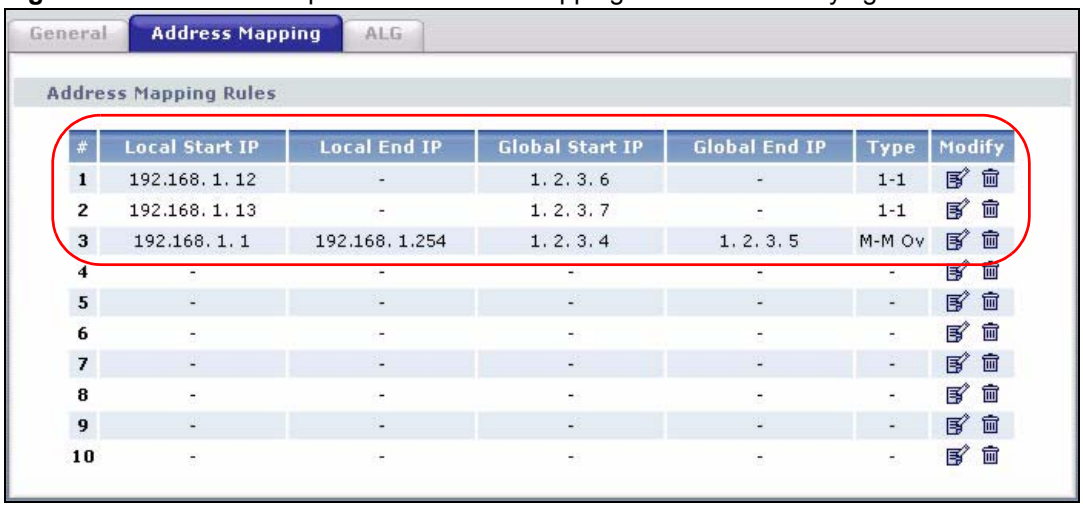
2.6 Using NAT with Multiple Game Players

If two users (behind the ZyXEL Device) want to connect to the same server to play online games at the same time, but the server does not allow more than one login from the same IP address, you can configure a many-to-many rule instead of a many-to-one rule.

In this example, you have four static IP addresses (1.2.3.4 to 1.2.3.7) from your ISP. After you set up your WAN connection (see Section 2.5.2 on page 59), use the **NAT > Address Mapping** screen to map the third and forth public IP addresses to the mail server (192.168.1.12) and web server (192.168.1.13) respectively. The first and second public IP addresses are mapped to other outgoing LAN traffic. See Section 2.5.3 on page 62 for more information about IP address mapping.

When you finish configuration, the screen looks as shown.

Figure 46 Tutorial Example: NAT Address Mapping Done: Game Playing



To allow traffic from the WAN to be forwarded through the ZyXEL Device, you must also create a firewall rule. Refer to Section 2.5.5 on page 67 for more information.

2.7 How to Make a VoIP Call

You can register a SIP account with the SIP server and make voice calls over the Internet to another VoIP device. You can also make a peer-to-peer call to a VoIP device directly without a registered SIP account or SIP server. You must know the peer device's IP address or domain name.

2.7.1 VoIP Calls With a Registered SIP Account

To use a registered SIP account, you should have applied for a SIP account with the VoIP service provider and got account information from your provider.

This section shows you examples of how to register your SIP account on the ZyXEL Device and make Internet calls.

The following table shows the SIP account and SIP server address provided by your service provider.

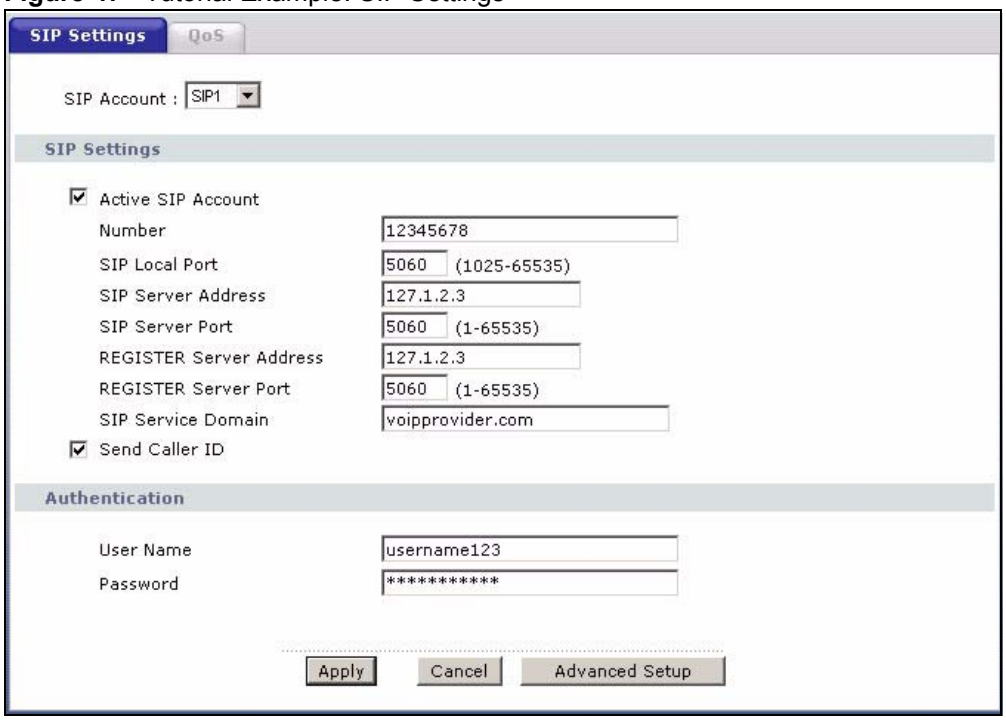
SIP Account	12345678@voipprovider.com
SIP Server Address	127.1.2.3
User Name	username123
Password	password123

2.7.1.1 SIP Account Registration

Follow the steps below to register and activate your SIP account.

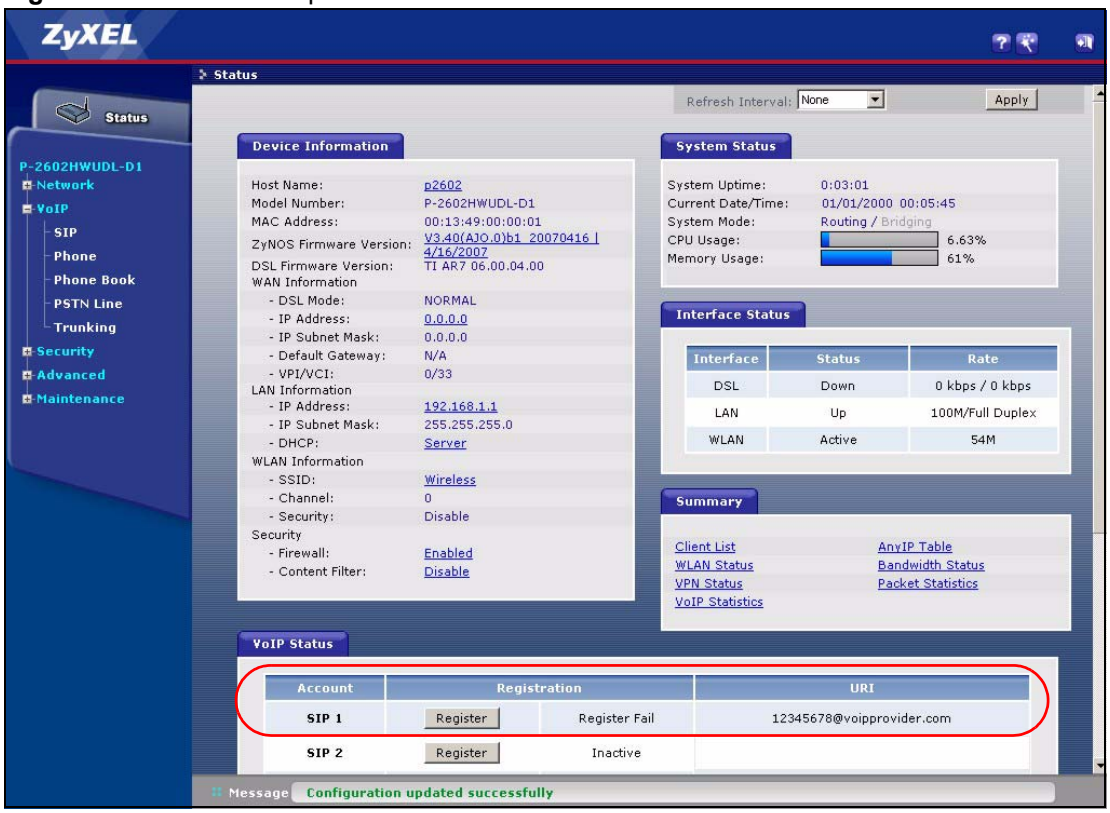
1. Make sure your ZyXEL Device is connected to the Internet.
2. Open the web configurator and go to **VoIP > SIP**.
3. Select **SIP1** to configure the first SIP account.
4. Select the checkbox to enable the SIP account on the ZyXEL Device.
5. Enter the SIP number ("12345678" in this example) which is the part before the @ symbol in your SIP account.
6. Enter the SIP server address ("127.1.2.3" in this example).
7. Repeat the SIP server address in the **REGISTER Server Address** field.
8. Enter the SIP server domain ("voipprovider.com" in this example) which is the part after the @ symbol in your SIP account.
9. Enter your user name and password. Click **Apply** to save your changes.

Figure 47 Tutorial Example: SIP Settings



10 Go to the **Status** screen to check if your SIP account has been registered successfully. If registration failed, check your SIP settings and click **Register** to register your SIP account again.

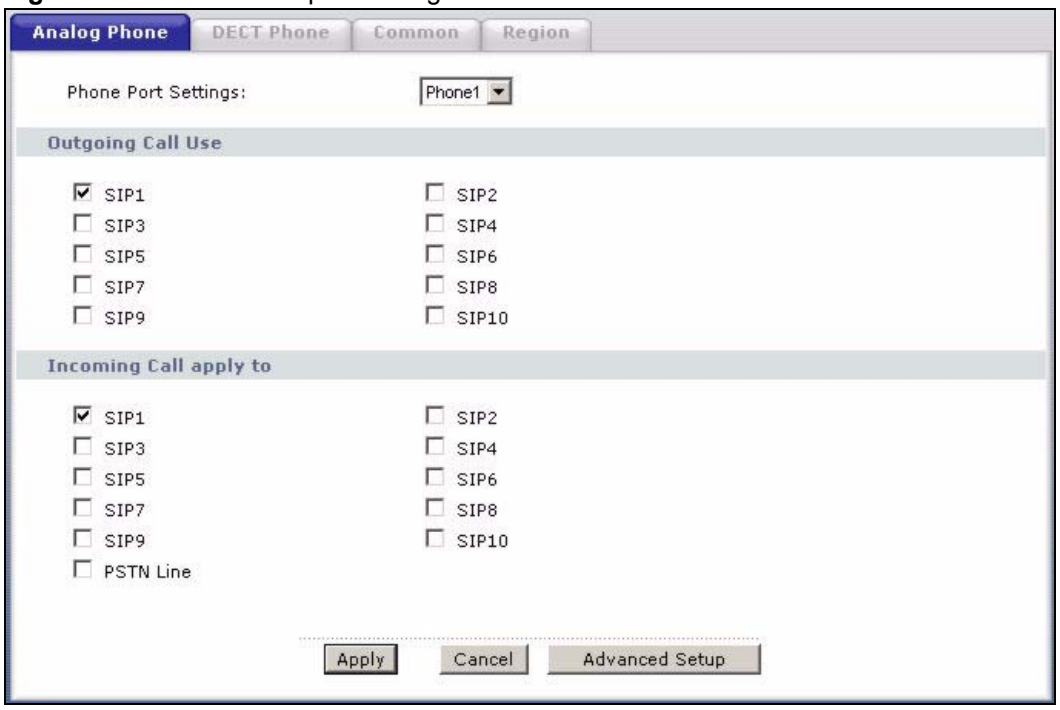
Figure 48 Tutorial Example: Status



2.7.1.2 Analog Phone Configuration

1. Click **VoIP > Phone** to open the **Analog Phone** screen.
2. Select **Phone 1** to configure the first phone port.
3. Select the **SIP1** checkbox in the **Outgoing Call Use** section to have the phone (connected to the first phone port) use the registered SIP1 account to make outgoing calls.
4. Select the **SIP1** checkbox in the **Incoming Call apply to** section to have the phone (connected to the first phone port) receive phone calls for the SIP1 account.
5. Click **Apply** to save your changes.

Figure 49 Tutorial Example: Analog Phone



2.7.1.3 Making a VoIP Call

1. Make sure you connect a telephone to the first phone port on the ZyXEL Device.
2. Make sure the ZyXEL Device is on and connected to the Internet.
3. Pick up the phone receiver.
4. Dial the VoIP phone number you want to call.

2.7.2 VoIP Calls Without a SIP Server

To make a call directly to a peer VoIP device over the Internet, you need to know the IP address or domain name of the peer device. In a peer-to-peer call, there is no VoIP service provider involved. You don't need to register a SIP account successfully with the SIP server. Therefore, the SIP account does not need to be a real SIP account, but you should still activate the SIP account and configure its number and map it to a phone port.

This section shows you examples of how to make peer-to-peer calls.

The following table shows the information you need in this example.

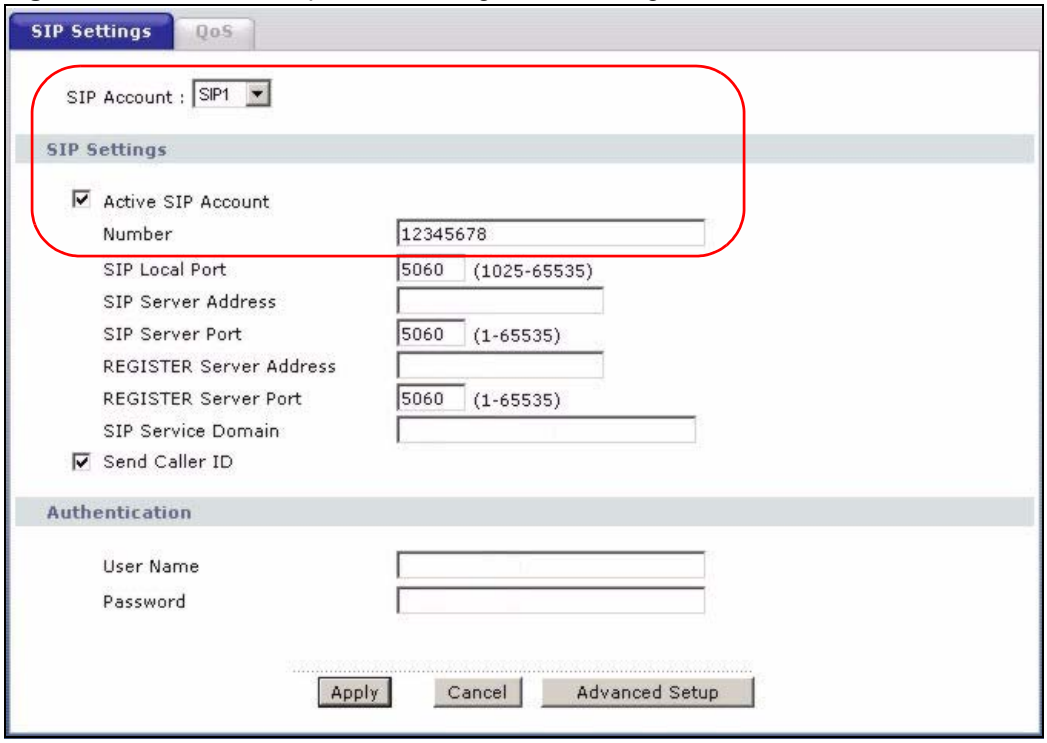
SIP Number of the Phone Connected to the ZyXEL Device	12345678
Peer Device's IP Address or URL	10.1.2.3
Peer Device's SIP Number	22222222

2.7.2.1 SIP Account Configuration

If you didn't register a SIP account before and want to make only peer-to-peer VoIP calls, follow the steps below to configure an unregistered SIP account for the phone attached to the ZyXEL Device.

1. Click **VoIP > SIP**.
2. Select **SIP1** to configure the first SIP account.
3. Select the checkbox to enable the SIP account on the ZyXEL Device.
4. Enter the SIP number ("12345678" in this example) which you want to map to the phone attached to the ZyXEL Device.
5. Leave other fields blank or at the default
6. Click **Apply** to save your changes.

Figure 50 Tutorial Example: SIP Settings for an Unregistered SIP Account



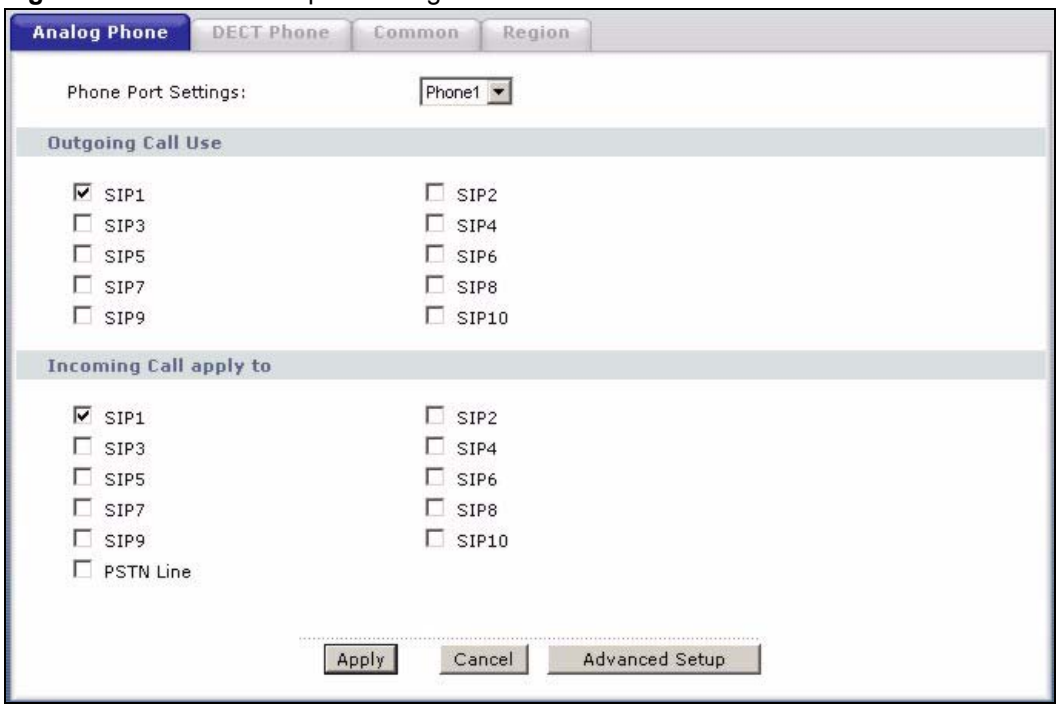
2.7.2.2 Analog Phone Configuration

1. Click **VoIP > Phone** to open the **Analog Phone** screen.
2. Select **Phone 1** to configure the first phone port.
3. Select the **SIP1** checkbox in the **Outgoing Call Use** section to have the phone (connected to the first phone port) use the SIP1 account to make outgoing calls.

4 Select the **SIP1** checkbox in the **Incoming Call apply to** section to have the phone (connected to the first phone port) receive phone calls for the SIP1 account.

5 Click **Apply** to save your changes.

Figure 51 Tutorial Example: Analog Phone



2.7.2.3 Peer-to-Peer Call Configuration

Follow the steps below to configure a speed dial entry for peer-to-peer calls.

1 Open the web configurator and go to **VoIP > Phone Book > Speed Dial**.

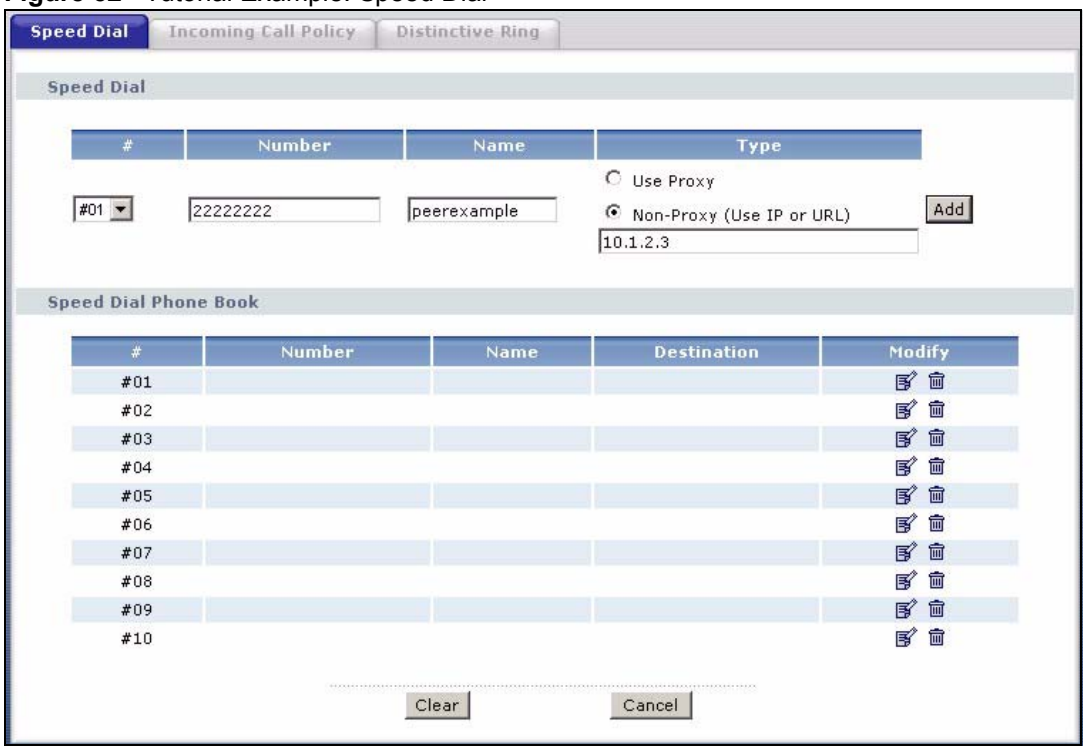
2 Select the speed-dial number (**#01** for example) you want to use for the peer device's phone number.

3 Enter the phone number ("22222222" in this example) and a descriptive name ("peerexample" for example) for the peer device.

4 Select **Non-Proxy (Use IP or URL)** and enter the peer device's IP address or domain name ("10.1.2.3" in this example).

5 Click **Add** to save a new entry in the speed dial phone book.

Figure 52 Tutorial Example: Speed Dial



2.7.2.4 Making a Peer-to-Peer VoIP Call

1. Make sure you connect a telephone to the first phone port on the ZyXEL Device.
2. Make sure the ZyXEL Device is on and connected to the Internet.
3. Pick up the phone receiver.
4. Dial #01 to make a peer-to-peer call to the peer device. You need to press the # (pound) key followed by the 0 and 1 keys.

3

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 453 if you need to make sure these functions are allowed in Internet Explorer.

3.1.1 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. The default password (“1234”) displays in non-readable characters. If you haven’t changed the password yet, you can just click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 53 Password Screen

5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 54 Change Password Screen

ZyXEL
Use this screen to change the password.
Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.
Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password
New Password:
Retype to Confirm:
Apply
Ignore

6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device.

Figure 55 Replace Certificate Screen

ZyXEL
Replace Factory Default Certificate
The factory default certificate is common to all ZyXEL models. Click Apply to create a certificate using your ZyXEL's MAC address that will be specific to this device.
Apply
Ignore

7 A screen displays to let you choose whether to go to the wizard or the advanced screens.

- Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears after you click **Apply**. See Chapter 4 on page 91 for more information.
- Click **Go to Advanced setup** if you want to configure features that are not available in the wizards. Select the check box if you always want to go directly to the advanced screens. The main screen appears after you click **Apply**. See Section 3.2 on page 84 for more information.
- Click **Exit** if you want to log out.

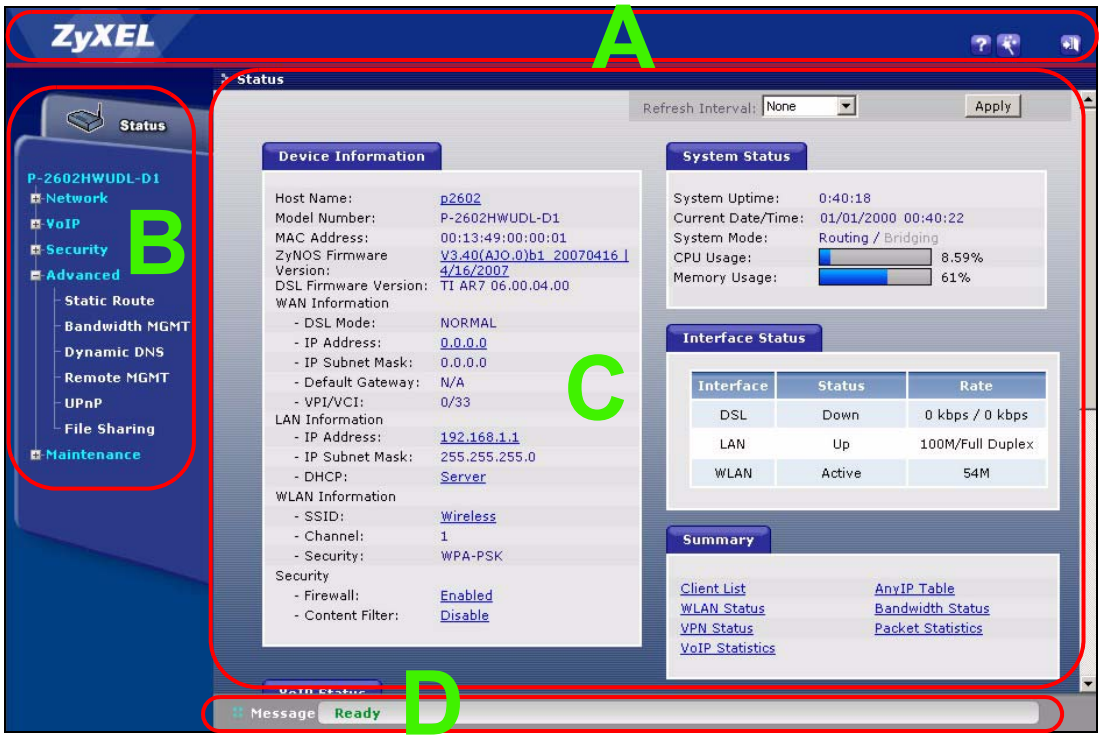
For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

Figure 56 Wizard or Advanced Screen

ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Click here to always start with the Advanced setup.
Apply
Exit

3.2 Web Configurator Main Screen

Figure 57 Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

3.2.1 Title Bar

The title bar allows you to change the language and provides some icons in the upper right corner.

The icons provide the following functions.

Table 3 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Help: Click this icon to open up help screens.
	Wizards: Click this icon to go to the configuration wizards. See Chapter 4 on page 91 for more information.
	Logout: Click this icon to log out of the web configurator.

3.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following tables describe each menu item.

Table 4 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
	WAN Backup Setup	Use this screen to configure a backup gateway.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.
Wireless LAN	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	OTIST	Use this screen to assign your wireless security settings to wireless clients.
	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific wireless clients or exclude specific wireless clients from accessing the ZyXEL Device.
	QoS	WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	ALG	Use this screen to enable or disable SIP ALG.
VoIP		
SIP	SIP Settings	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	QoS	Use this screen to configure your ZyXEL Device's Quality of Service settings for VoIP.
Phone	Analog Phone	Use this screen to set which phone ports use which SIP accounts.
	DECT Phone	Use this screen to enable your DECT phone base station and set up a secure password for DECT phone registration.
	Common	Use this screen to configure general phone port settings.
	Region	Use this screen to select your location and call service mode.

Table 4 Navigation Panel Summary

LINK	TAB	FUNCTION
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
	Incoming Call Policy	Use this screen to configure call-forwarding.
	Distinctive Ring	Use this screen to configure ring tone behavior based on the origin of incoming calls.
PSTN Line	General	Use this screen to configure your ZyXEL Device's settings for PSTN calls.
Trunking	General	Use this screen to enable trunking on your ZyXEL Device.
	Peer Call	Use this screen to configure peer device authentication for trunking calls.
	Call Rule	Use this screen to configure forwarding rules on your ZyXEL Device for trunking calls.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/ add a firewall rule.
	Threshold	Use this screen to configure the thresholds for determining when to drop sessions that do not become fully established.
Content Filter	Keyword	Use this screen to block access to web sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for your device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering.
VPN	Setup	Use this screen to configure each VPN tunnel.
	Monitor	Use this screen to look at the current status of each VPN tunnel.
	VPN Global Setting	Use this screen to allow NetBIOS traffic through VPN tunnels.
Certificates	My Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
	Trusted CAs	Use this screen to save CA certificates to the ZyXEL Device.
	Trusted Remote Hosts	Use this screen to import self-signed certificates.
	Directory Servers	Use this screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).
Advanced		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Bandwidth MGMT	General	Use this screen to configure bandwidth management on an interface.
	Rule Setup	Use this screen to define a bandwidth rule.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.

Table 4 Navigation Panel Summary

LINK	TAB	FUNCTION
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP	General	Use this screen to turn UPnP on or off.
File Sharing	Server Configuration	Use this screen to enable file sharing via the ZyXEL Device.
	User Configuration	Use this screen to setup a user's name and password for secure access to your shared files.
	Share Configuration	Use this screen to view or configure the share directories (folders) on the ZyXEL Device.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	DSL Line	These screen displays information to help you identify problems with the DSL connection.

3.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 7 on page 117 for more information about the **Status** screen.

3.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

PART II
Wizard

Internet and Wireless Setup Wizard (91)
VoIP Wizard And Example (105)
Bandwidth Management Wizard (111)

4

Internet and Wireless Setup Wizard

This chapter provides information on the Wizard Setup screens for Internet access in the web configurator.

4.1 Introduction

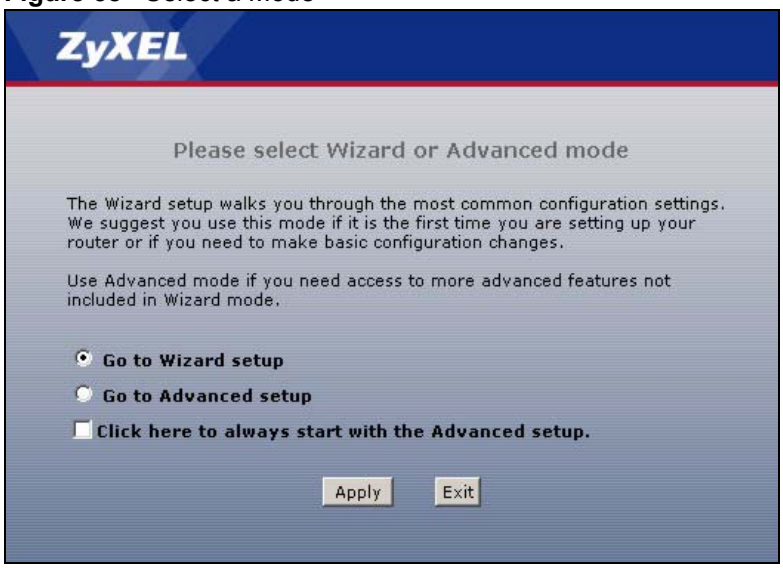
Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

See the advanced menu chapters for background information on these fields.

4.2 Internet Access Wizard Setup

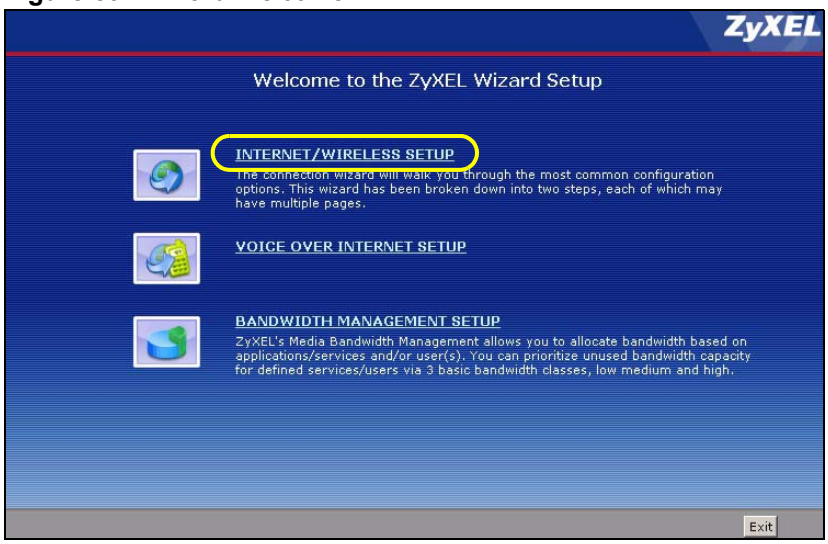
1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon ( ) in the top right corner of the web configurator to go to the wizards.

Figure 58 Select a Mode


ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Click here to always start with the Advanced setup.
Apply
Exit

2 Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access and wireless connection.

Figure 59 Wizard Welcome


ZyXEL
Welcome to the ZyXEL Wizard Setup
INTERNET/WIRELESS SETUP
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.
VOICE OVER INTERNET SETUP
BANDWIDTH MANAGEMENT SETUP
ZyXEL's Media Bandwidth Management allows you to allocate bandwidth based on applications/services and/or user(s). You can prioritize unused bandwidth capacity for defined services/users via 3 basic bandwidth classes, low medium and high.
Exit

3 Your ZyXEL device attempts to detect your DSL connection and your connection type.

3a The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to return to the wizard welcome screen. If you still cannot connect, click **Manually configure your Internet connection**. Follow the directions in the wizard and enter your Internet setup information as provided to you by your ISP. See Section 4.2.1 on page 94 for more details.

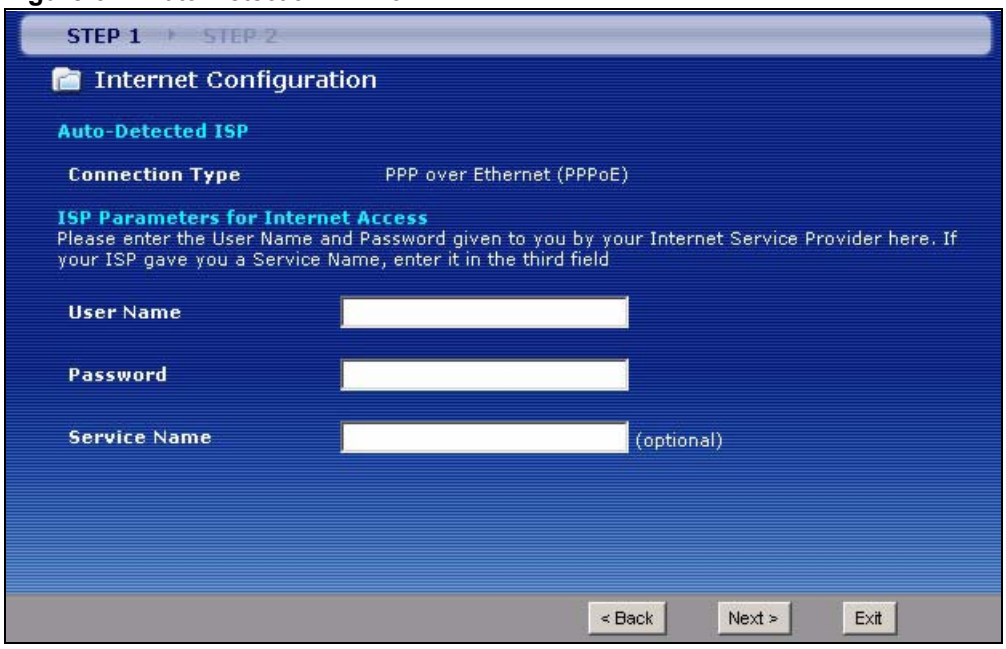
If you would like to skip your Internet setup and configure the wireless LAN settings, leave **Yes** selected and click **Next**.

Figure 60 Auto Detection: No DSL Connection

STEP 1
STEP 2
Internet Configuration
No DSL connection
Your router has not established a DSL connection to your local exchange. The DSL light on the router will blink while it is trying to connect, and stay on if it connects successfully.
Restart the Internet/Wireless Setup Wizard
Manually configure your Internet connection
Continue to Wireless Setup wizard? Yes No
Next >
Exit

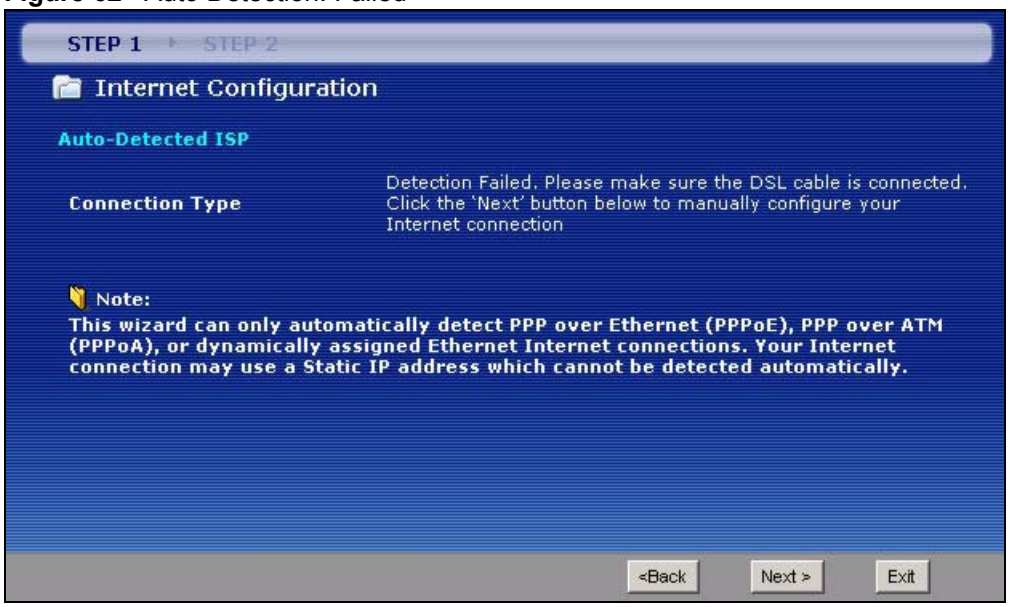
3b The following screen displays if a PPPoE or PPPoA connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP. Then click **Next** and see Section 4.3 on page 99 for wireless connection wizard setup.

Figure 61 Auto-Detection: PPPoE


STEP 1
STEP 2
Internet Configuration
Auto-Detected ISP
Connection Type
PPP over Ethernet (PPPoE)
ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field
User Name
Password
Service Name
(optional)
< Back
Next >
Exit

3c The following screen appears if the ZyXEL device detects a connection but not the connection type. Click **Next** and refer to Section 4.2.1 on page 94 on how to manually configure the ZyXEL Device for Internet access.

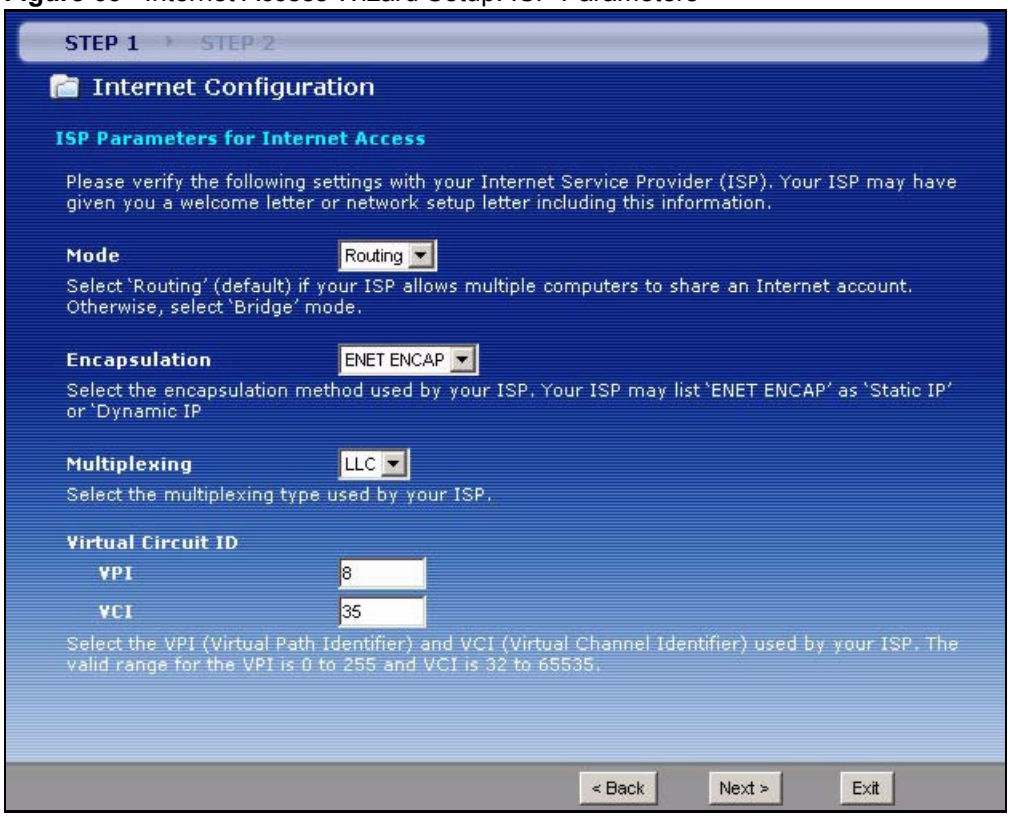
Figure 62 Auto Detection: Failed


STEP 1
STEP 2
Internet Configuration
Auto-Detected ISP
Connection Type
Detection Failed. Please make sure the DSL cable is connected. Click the 'Next' button below to manually configure your Internet connection
Note:
This wizard can only automatically detect PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), or dynamically assigned Ethernet Internet connections. Your Internet connection may use a Static IP address which cannot be detected automatically.
<Back
Next >
Exit

4.2.1 Manual Configuration

1 If the ZyXEL Device fails to detect your DSL connection type but the physical line is connected, enter your Internet access information in the wizard screen exactly as your service provider gave it to you. Leave the defaults in any fields for which you were not given information.

Figure 63 Internet Access Wizard Setup: ISP Parameters


STEP 1
STEP 2
Internet Configuration
ISP Parameters for Internet Access
Please verify the following settings with your Internet Service Provider (ISP). Your ISP may have given you a welcome letter or network setup letter including this information.
Mode
Routing
Select 'Routing' (default) if your ISP allows multiple computers to share an Internet account. Otherwise, select 'Bridge' mode.
Encapsulation
ENET ENCAP
Select the encapsulation method used by your ISP. Your ISP may list 'ENET ENCAP' as 'Static IP' or 'Dynamic IP
Multiplexing
LLC
Select the multiplexing type used by your ISP.
Virtual Circuit ID
VPI
8
VCI
35
Select the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) used by your ISP. The valid range for the VPI is 0 to 255 and VCI is 32 to 65535.
< Back
Next >
Exit

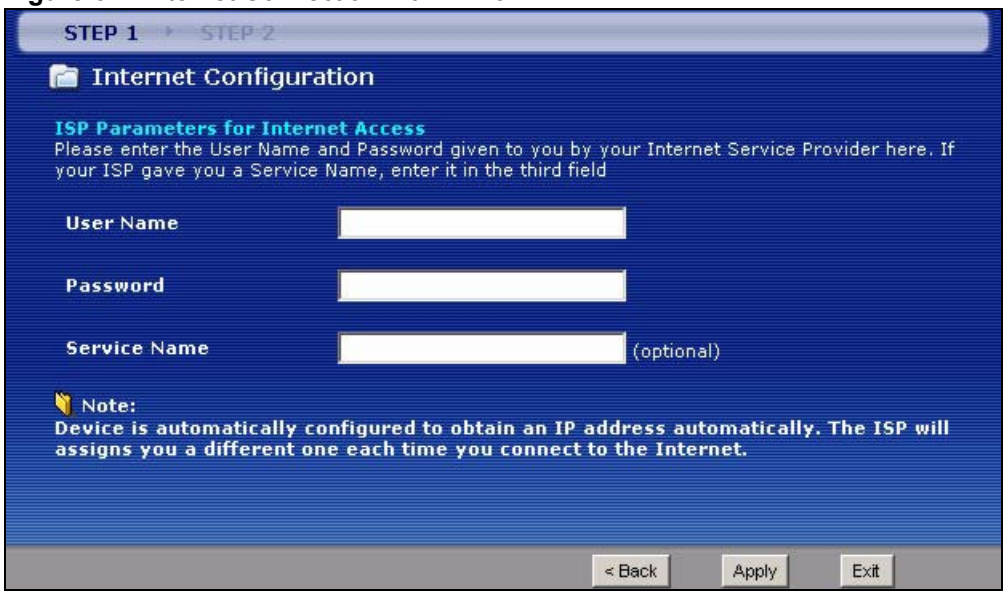
The following table describes the fields in this screen.

Table 5 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account. Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the ZyXEL Device.
Encapsulation	Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplexing	Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Back	Click **Back** to go back to the previous screen.
Next	Click **Next** to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click **Exit** to close the wizard screen without saving your changes.

2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue. See Section 4.3 on page 99 for wireless connection wizard setup

Figure 64 Internet Connection with PPPoE


STEP 1
STEP 2
Internet Configuration
ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field
User Name
Password
Service Name
(optional)
Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assigns you a different one each time you connect to the Internet.
< Back
Apply
Exit

The following table describes the fields in this screen.

Table 6 Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of your PPPoE service here.
Back	Click **Back** to go back to the previous wizard screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Exit	Click **Exit** to close the wizard screen without saving your changes.

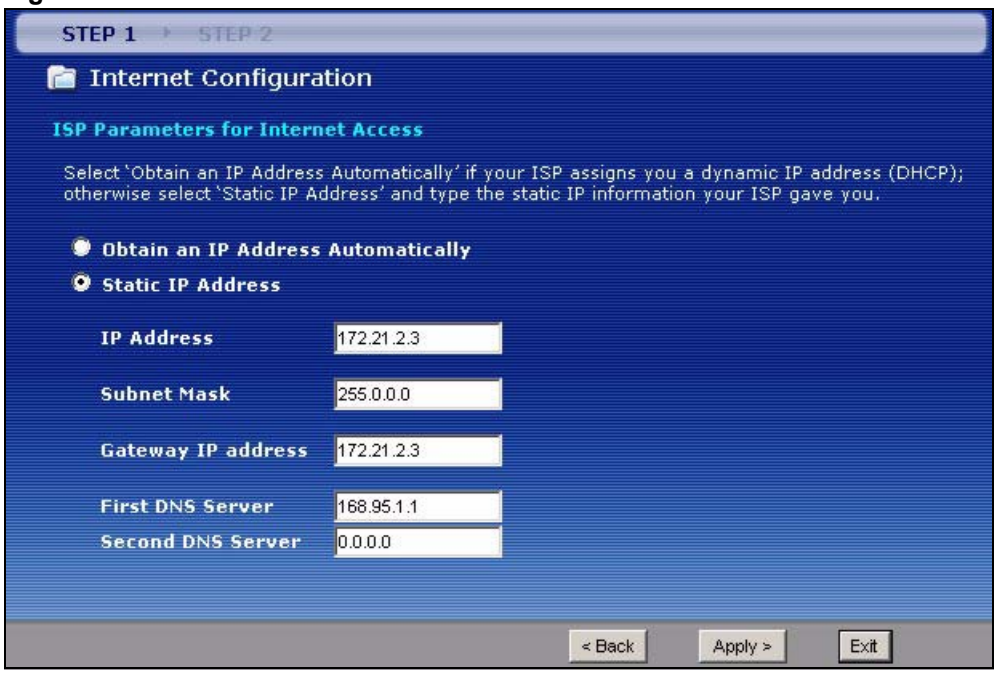
Figure 65 Internet Connection with RFC 1483

The following table describes the fields in this screen.

Table 7 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select **Routing** in the **Mode** field. Type your ISP assigned IP address in this field.
Back	Click **Back** to go back to the previous wizard screen.
Next	Click **Next** to continue to the next wizard screen.
Exit	Click **Exit** to close the wizard screen without saving your changes.

Figure 66 Internet Connection with ENET ENCAP



The following table describes the fields in this screen.

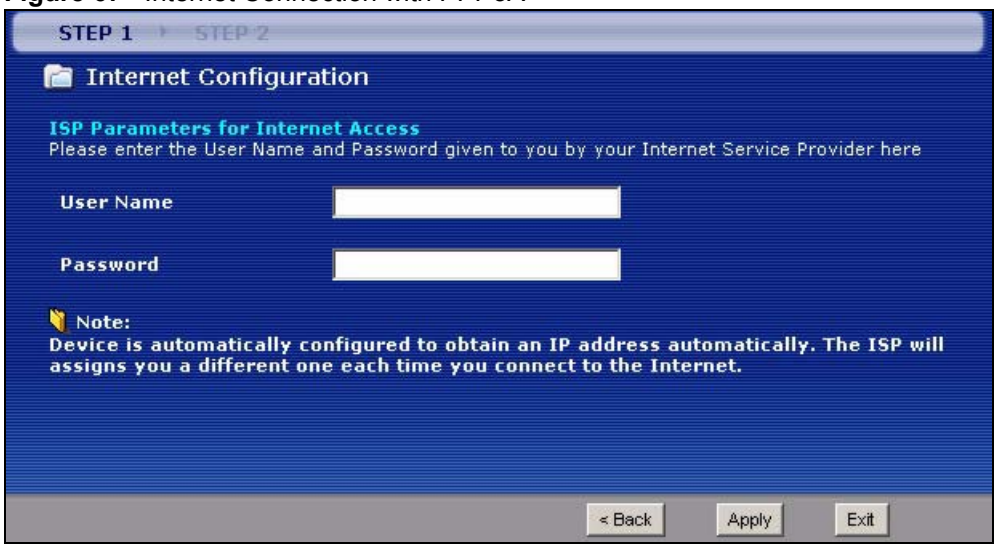
Table 8 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address.
Static IP Address	Select **Static IP Address** if your ISP gave you an IP address to use.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click **Back** to go back to the previous wizard screen.

Table 8 Internet Connection with ENET ENCAP (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Exit	Click **Exit** to close the wizard screen without saving your changes.

Figure 67 Internet Connection with PPPoA


STEP 1
STEP 2
Internet Configuration
ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here
User Name
Password
Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assigns you a different one each time you connect to the Internet.
< Back
Apply
Exit

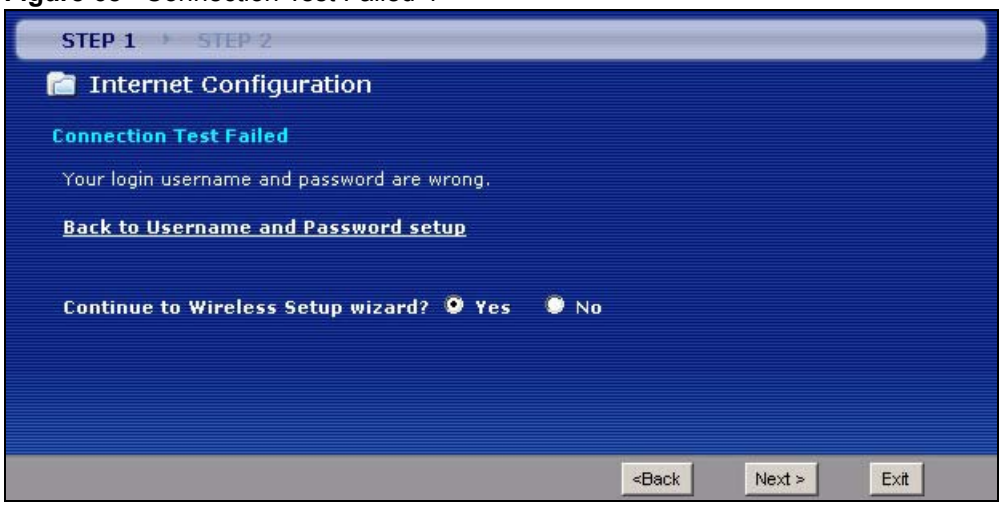
The following table describes the fields in this screen.

Table 9 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click **Back** to go back to the previous wizard screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Exit	Click **Exit** to close the wizard screen without saving your changes.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.

Figure 68 Connection Test Failed-1



- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

Figure 69 Connection Test Failed-2.

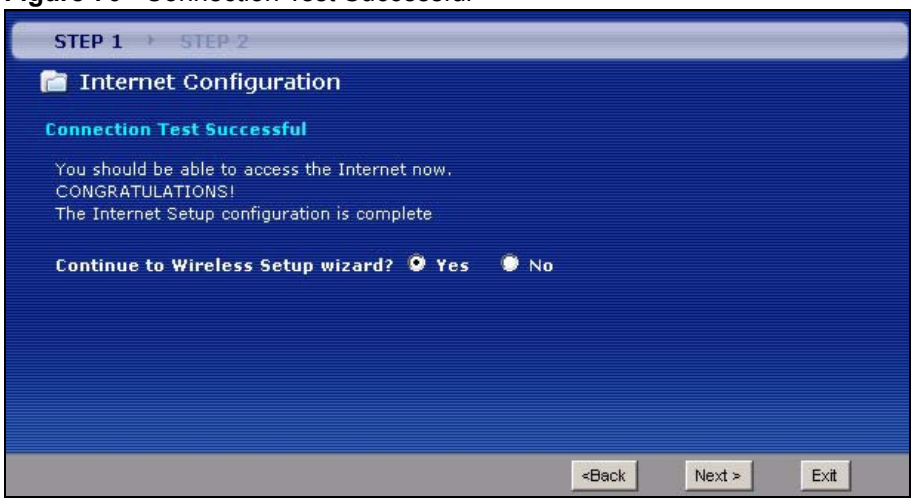
STEP 1
STEP 2
Internet Configuration
Connection Test Failed
Cannot access the Internet, please check your ISP account is active and that the settings you entered in the wizard are correct. If you still have problems, please contact customer support.
Restart the Internet/Wireless Setup Wizard
Continue to Wireless Setup wizard? Yes No
<Back
Next >
Exit

4.3 Wireless Connection Wizard Setup

After you configure the Internet access information, use the following screens to set up your wireless LAN.

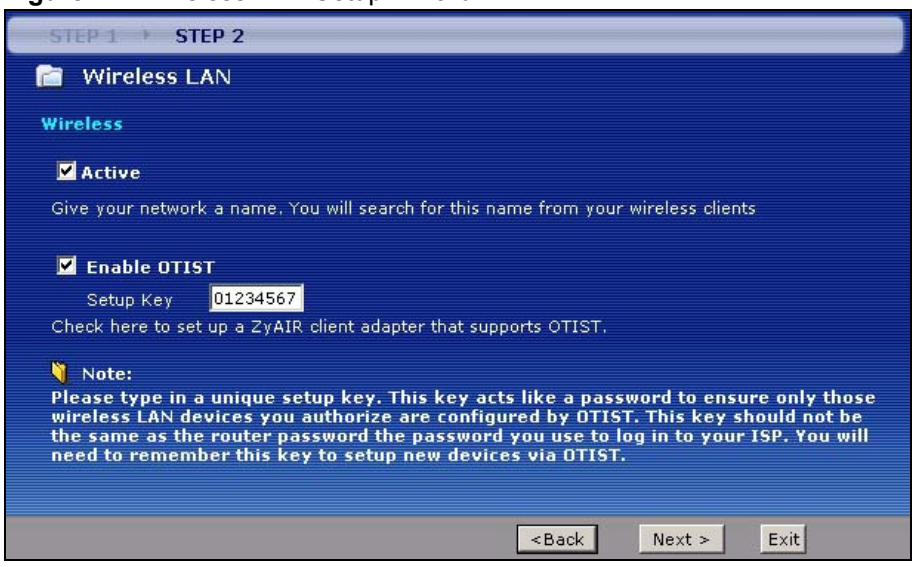
1 Select **Yes** and click **Next** to configure wireless settings. Otherwise, select **No** and skip to Step 6.

Figure 70 Connection Test Successful



2 Use this screen to activate the wireless LAN and OTIST. Click **Next** to continue.

Figure 71 Wireless LAN Setup Wizard 1


STEP 1
STEP 2
Wireless LAN
Wireless
Active
Give your network a name. You will search for this name from your wireless clients
Enable OTIST
Setup Key
01234567
Check here to set up a ZyAIR client adapter that supports OTIST.
Note:
Please type in a unique setup key. This key acts like a password to ensure only those wireless LAN devices you authorize are configured by OTIST. This key should not be the same as the router password the password you use to log in to your ISP. You will need to remember this key to setup new devices via OTIST.
<Back
Next >
Exit

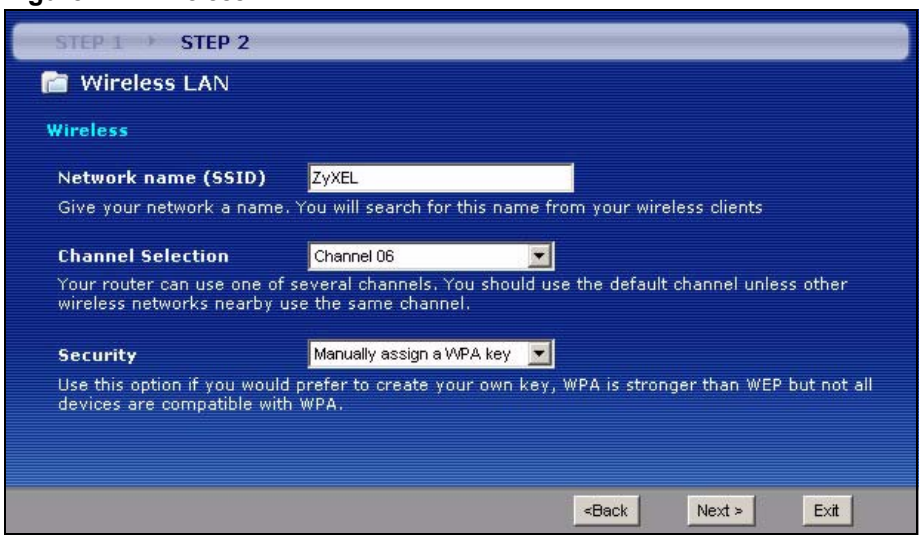
The following table describes the labels in this screen.

Table 10 Wireless LAN Setup Wizard 1

LABEL	DESCRIPTION
Active	Select the check box to turn on the wireless LAN.
Enable OTIST	Select the check box to enable OTIST if you want to transfer your ZyXEL Device's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You must also activate and start OTIST on the wireless client at the same time. The process takes three minutes to complete.
Setup Key	Type an OTIST **Setup Key** of up to eight ASCII characters in length. Be sure to use the same OTIST **Setup Key** on the ZyXEL Device and wireless clients.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3 Configure your wireless settings in this screen. Click **Next**.

Figure 72 Wireless LAN


STEP 1
STEP 2
Wireless LAN
Wireless
Network name (SSID)
ZyXEL
Give your network a name. You will search for this name from your wireless clients
Channel Selection
Channel 06
Your router can use one of several channels. You should use the default channel unless other wireless networks nearby use the same channel.
Security
Manually assign a WPA key
Use this option if you would prefer to create your own key, WPA is stronger than WEP but not all devices are compatible with WPA.
<Back
Next >
Exit

The following table describes the labels in this screen.

Table 11 Wireless LAN Setup Wizard 2

LABEL	DESCRIPTION
Network Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select **Automatically assign a WPA key (Recommended)** (only available if you enable OTIST) if you want OTIST to configure a WPA key for you. Select **Manually assign a WPA-PSK key** to configure a Pre-Shared Key (WPA-PSK). Choose this option only if your wireless clients support WPA. See Section 4.3.1 on page 102 for more information. Select **Manually assign a WEP key** to configure a WEP Key. See Section 4.3.2 on page 102 for more information. Select **Disable wireless security** to have no wireless LAN security configured and your network is accessible to any wireless networking device that is within range.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

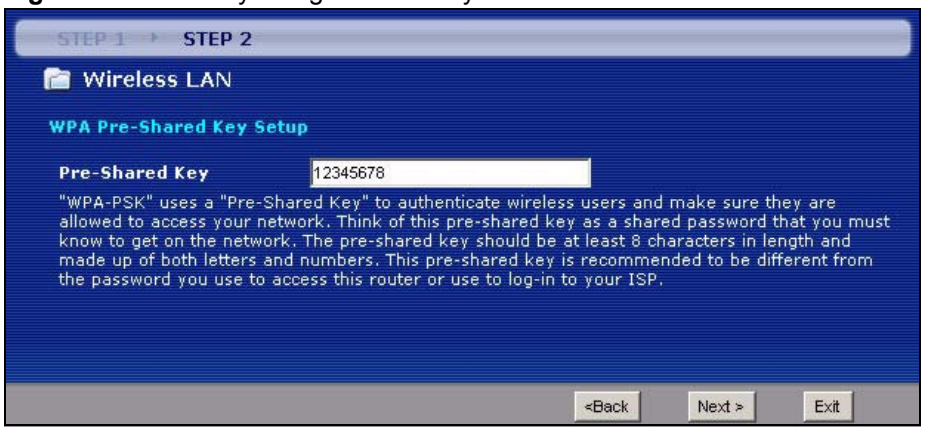
The wireless stations and ZyXEL Device must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) for wireless communication.

4 This screen varies depending on the security mode you selected in the previous screen. Fill in the field (if available) and click **Next**.

4.3.1 Manually Assign a WPA key

Choose **Manually assign a WPA key** in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 73 Manually Assign a WPA key


STEP 1
STEP 2
Wireless LAN
WPA Pre-Shared Key Setup
Pre-Shared Key
12345678
"WPA-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network. The pre-shared key should be at least 8 characters in length and made up of both letters and numbers. This pre-shared key is recommended to be different from the password you use to access this router or use to log-in to your ISP.
<Back
Next >
Exit

The following table describes the labels in this screen.

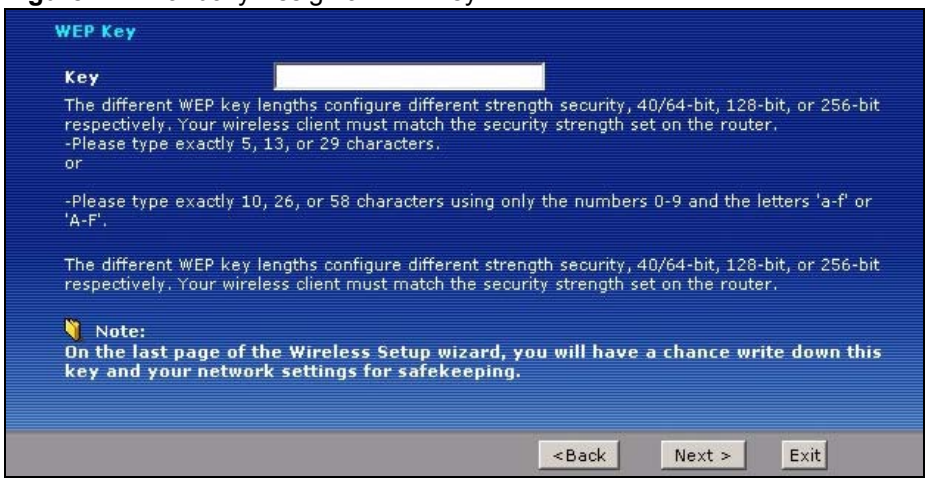
Table 12 Manually Assign a WPA key

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4.3.2 Manually Assign a WEP Key

Choose **Manually assign a WEP key** to setup WEP Encryption parameters.

Figure 74 Manually Assign a WEP key


WEP Key
Key
The different WEP key lengths configure different strength security, 40/64-bit, 128-bit, or 256-bit respectively. Your wireless client must match the security strength set on the router.
-Please type exactly 5, 13, or 29 characters.
or
-Please type exactly 10, 26, or 58 characters using only the numbers 0-9 and the letters 'a-f' or 'A-F'.
The different WEP key lengths configure different strength security, 40/64-bit, 128-bit, or 256-bit respectively. Your wireless client must match the security strength set on the router.
Note:
On the last page of the Wireless Setup wizard, you will have a chance write down this key and your network settings for safekeeping.
<Back
Next >
Exit

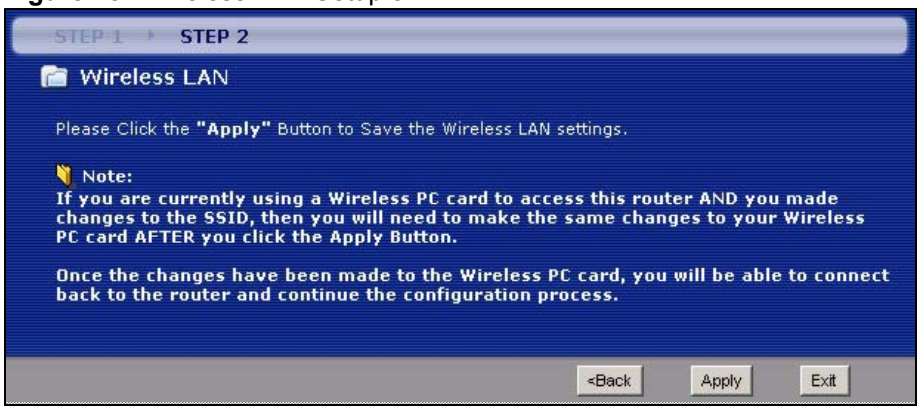
The following table describes the labels in this screen.

Table 13 Manually Assign a WEP key

LABEL	DESCRIPTION
Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Enter any 5, 13 or 29 ASCII characters or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

5 Click **Apply** to save your wireless LAN settings.

Figure 75 Wireless LAN Setup 3


STEP 1
STEP 2
Wireless LAN
Please Click the "Apply" Button to Save the Wireless LAN settings.
Note:
If you are currently using a Wireless PC card to access this router AND you made changes to the SSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Apply Button.
Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.
<Back
Apply
Exit

6 Use the read-only summary table to check whether what you have configured is correct. Click **Finish** to complete and save the wizard setup.

No wireless LAN settings display if you chose not to configure wireless LAN settings.

Figure 76 Internet Access and WLAN Wizard Setup Complete

CONGRATULATIONS!
The Internet/Wireless Setup configuration is complete. Here is your current settings.
Internet Settings
Mode : Routing
Encapsulation : Enet Encap
Mutiplexing : VC
VPI/VCI : 0/33
Wireless LAN Settings
Network Name(SSID) : ZyXEL
Channel : 6
Security : Manually assigned a WEP key
Network Key(WEP Key) : 12345
Press "Finish" button to close this wizard, or click the following link to open other pages.page.
Return to Wizard Main Page
View device Status
<Back
Finish

7 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

5

VoIP Wizard And Example

This chapter shows you how to configure your SIP account(s) and make a VoIP phone call.

5.1 Introduction

The ZyXEL Device has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog telephone to make Internet calls. You can configure the ZyXEL Device to use up to two SIP based VoIP accounts.

This section describes how you can set up your ZyXEL Device to call someone who is also using a VoIP device. Make sure your telephone is connected to the **Phone 1** port before you start with our example.

In the following figure, **A** represents your phone and **B** represents the phone of the person you would like to call.

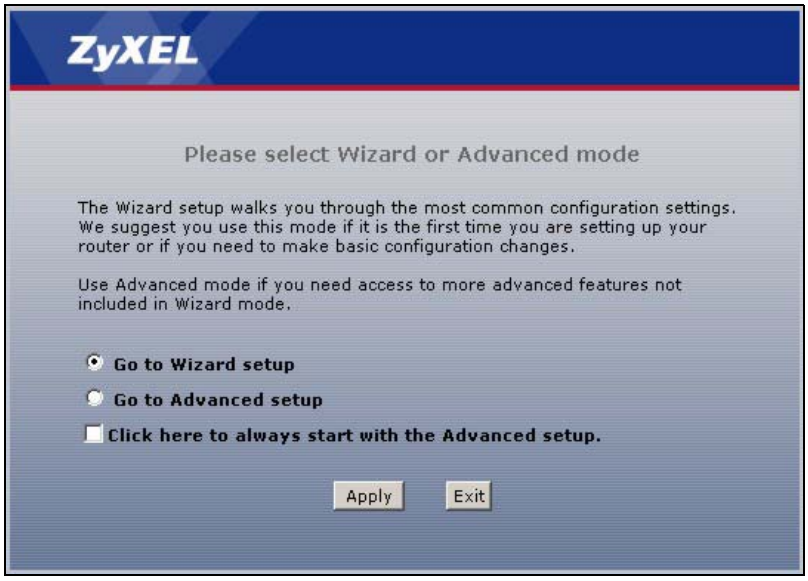
Figure 77 VoIP Phone Calls

In order to make VoIP calls you need to register at least one SIP account on your ZyXEL Device. You can register your SIP account in the **VOICE OVER INTERNET SETUP** wizard.

5.2 VoIP Wizard Setup

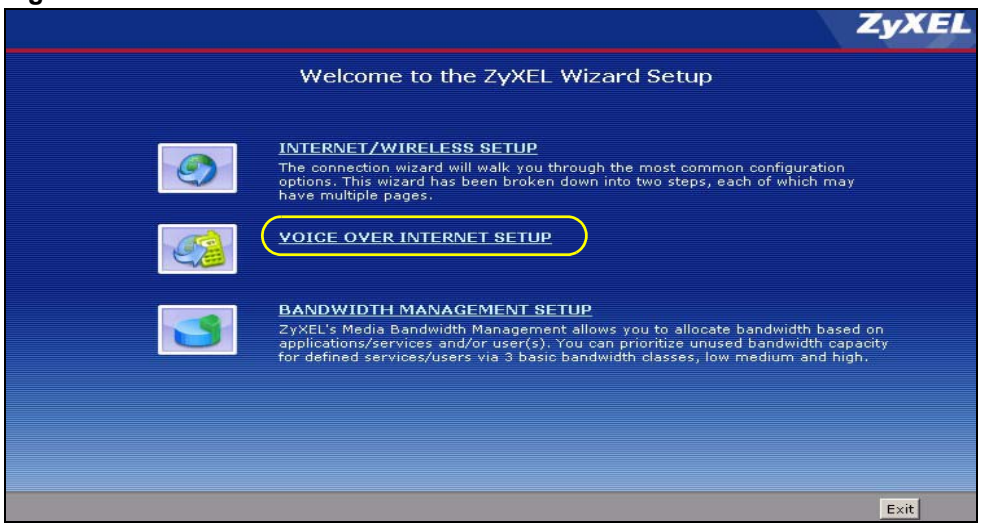
1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon ( ) in the top right corner of the web configurator to display the wizard main screen.

Figure 78 Select a Mode


ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Click here to always start with the Advanced setup.
Apply
Exit

2 Click **VOICE OVER INTERNET SETUP** to configure your SIP settings.

Figure 79 Wizard: Welcome


ZyXEL
Welcome to the ZyXEL Wizard Setup
INTERNET/WIRELESS SETUP
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.
VOICE OVER INTERNET SETUP
BANDWIDTH MANAGEMENT SETUP
ZyXEL's Media Bandwidth Management allows you to allocate bandwidth based on applications/services and/or user(s). You can prioritize unused bandwidth capacity for defined services/users via 3 basic bandwidth classes, low medium and high.
Exit

3 Fill in the **VOICE OVER INTERNET SETUP** wizard screen with the information provided by your VoIP service provider. Your VoIP service provider supplies you with the following information. When you are finished, click **Apply**.

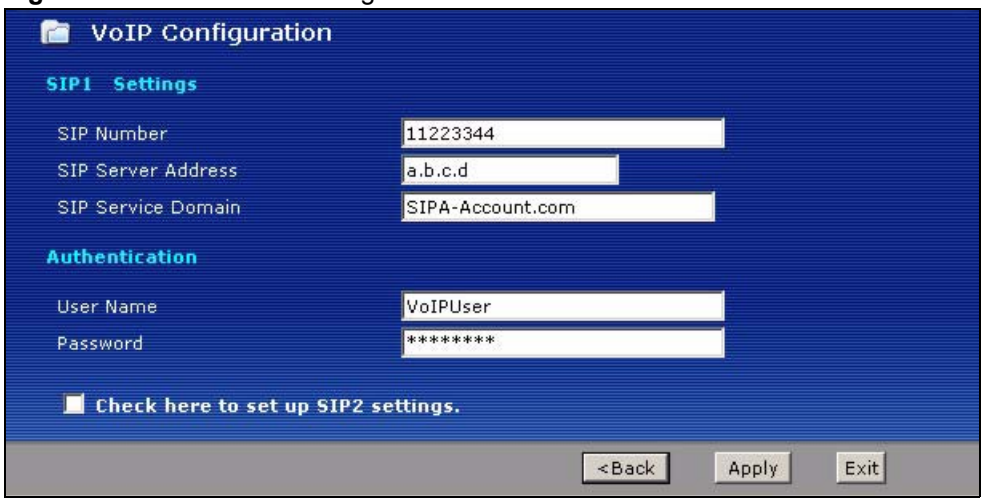
Table 14 Sample SIP Account Information

INFORMATION FROM VOIP SERVICE PROVIDER	EXAMPLE VALUES	DESCRIPTION
SIP account address	11223344@SIPA-Account.com	**11223344** is your SIP number. This is the part that comes before the "@" symbol in your SIP account address. **SIPA-Account.com** is your SIP server domain.
SIP server address	a.b.c.d	**a.b.c.d** is the IP address or domain name of your SIP server.

Table 14 Sample SIP Account Information

INFORMATION FROM VOIP SERVICE PROVIDER	EXAMPLE VALUES	DESCRIPTION
Username	VoIPUser	This is the username you use to login to your SIP account.
Password	Password	This is the password you use to login to your SIP account.

Figure 80 VoIP Wizard Configuration



The following table describes the labels in this screen.

Table 15 VoIP Wizard Configuration

LABEL	DESCRIPTION
SIP Number	Enter your SIP number in this field. Use the number or text that comes before the @ symbol in a SIP account. If your SIP account is 11223344@SIPA-Account.com, your SIP number is “11223344”. You can use up to 127 ASCII characters.
SIP Server Address	Type the IP address or domain name of the SIP server in this field. It doesn’t matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a SIP account like 11223344@SIPA-Account.com). You can use up to 127 ASCII Extended set characters.
User Name	This is the name used to register this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Check here to set up SIP2 settings.	This screen configures SIP account 1. Select the check box if you have a second SIP account that you want to use. You will need to configure the same fields for the second SIP account. Note: If you configure more than one SIP account, you need to configure **Analog Phone** settings to distinguish between the two accounts when you make and receive phone calls.

Table 15 VoIP Wizard Configuration

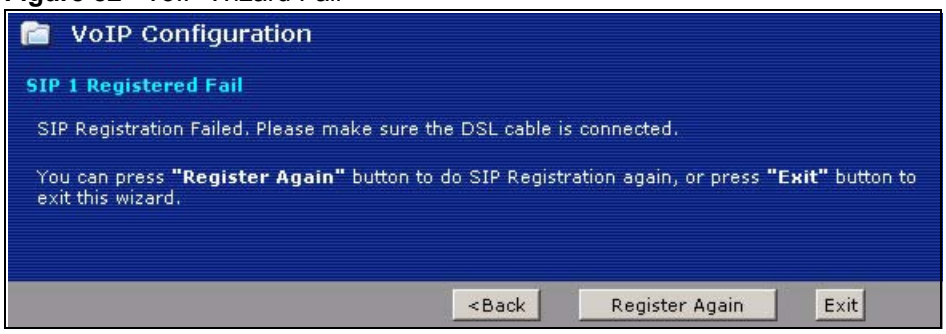
LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to complete the wizard setup and save your configuration.
Exit	Click **Exit** to close the wizard without saving your settings.

4 Your ZyXEL Device will attempt to register your SIP account with your VoIP service provider. When your account is registered your **PHONE** light will come on and you are ready to make and receive VoIP phone calls.

Figure 81 SIP Registration Test

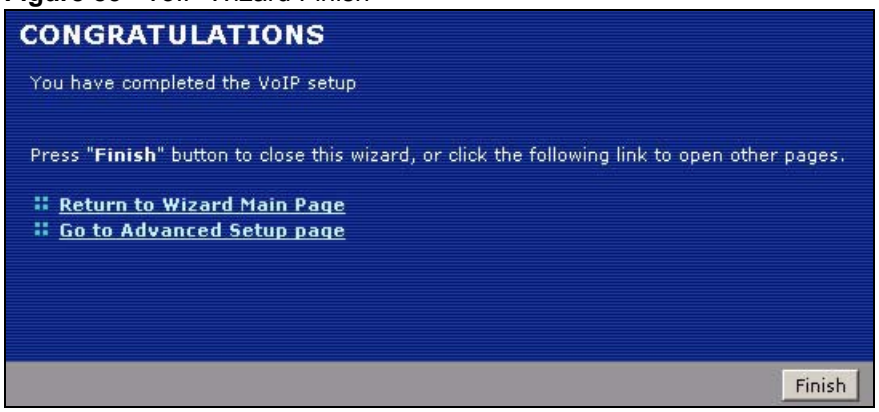
5 This screen displays if SIP account registration fails. If your DSL cable was disconnected, you can try connecting it. Then wait a few seconds and click **Register Again**. If your Internet connection was already working, you can click **Back** and try re-entering your SIP account settings.

Figure 82 VoIP Wizard Fail


VoIP Configuration
SIP 1 Registered Fail
SIP Registration Failed. Please make sure the DSL cable is connected.
You can press "Register Again" button to do SIP Registration again, or press "Exit" button to exit this wizard.
<Back
Register Again
Exit

6 This screen displays if your SIP account registration was successful. Click **Return to Wizard Main Page** if you want to use another configuration wizard. Click **Go to Advanced Setup page** or **Finish** to close the wizard and go to the main web configurator screens.

Figure 83 VoIP Wizard Finish


CONGRATULATIONS
You have completed the VoIP setup
Press "Finish" button to close this wizard, or click the following link to open other pages.
Return to Wizard Main Page
Go to Advanced Setup page
Finish

7 To call other VoIP users, you need to follow a similar process to ensure that their SIP account is registered and active. After it is registered, they need to provide you with their SIP number. You can use your VoIP service provider's dialing plan to call SIP numbers.

You can also use your VoIP service provider's dialing plan to call regular phone numbers. You dial a prefix number, provided to you by your VoIP service provider, followed by a regular phone number.

To find out more information about configuring your VoIP features and making non-VoIP calls see Chapter 12 on page 185.

6

Bandwidth Management Wizard

This chapter shows you how to configure basic bandwidth management using the wizard screens.

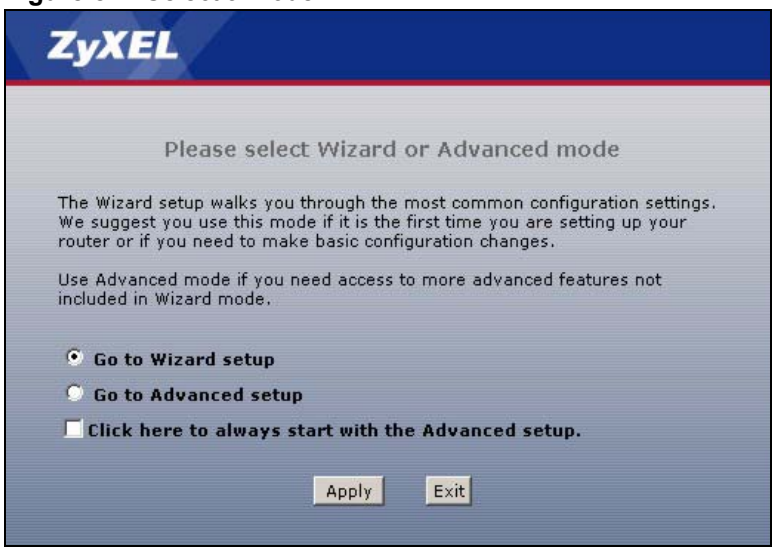
6.1 Introduction

Bandwidth management allows you to control the amount of bandwidth going out through the ZyXEL Device's WAN port and prioritize the distribution of the bandwidth according to service bandwidth requirements. This helps keep one service from using all of the available bandwidth and shutting out other users.

6.2 Bandwidth Management Wizard Setup

1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon ( ) in the top right corner of the web configurator to display the wizard main screen.

Figure 84 Select a Mode


ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Click here to always start with the Advanced setup.
Apply
Exit

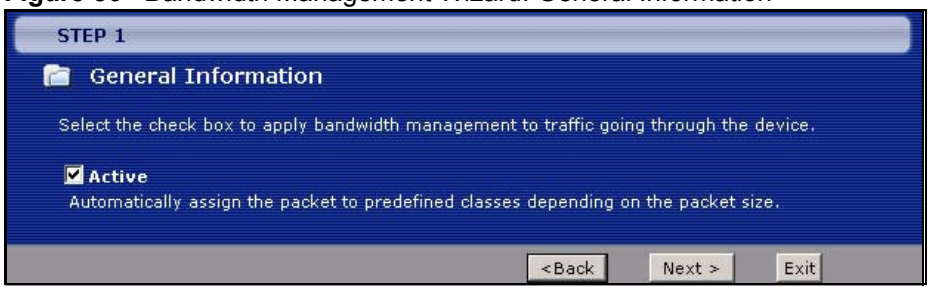
2 Click **BANDWIDTH MANAGEMENT SETUP**.

Figure 85 Wizard: Welcome

ZyXEL
Welcome to the ZyXEL Wizard Setup
INTERNET/WIRELESS SETUP
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.
VOICE OVER INTERNET SETUP
BANDWIDTH MANAGEMENT SETUP
ZyXEL's Media Bandwidth Management allows you to allocate bandwidth based on applications/services and/or user(s). You can prioritize unused bandwidth capacity for defined services/users via 3 basic bandwidth classes, low medium and high.
Exit

3 Select **Active** to allocate bandwidth to packets based on the packet size.

Figure 86 Bandwidth Management Wizard: General Information


STEP 1
General Information
Select the check box to apply bandwidth management to traffic going through the device.
Active
Automatically assign the packet to predefined classes depending on the packet size.
<Back
Next >
Exit

The following fields describe the label in this screen.

Table 16 Bandwidth Management Wizard: General Information

LABEL	DESCRIPTION
Active	Select the **Active** check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's WAN, LAN or WLAN port based on the packet size.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4 Follow the on-screen instructions and click **Finish** to complete the wizard setup and save your configuration.

Figure 87 Bandwidth Management Wizard: Complete

CONGRATULATIONS!
You have completed the Media Bandwidth Management setup. You can press "Finish" button to complete Bandwidth Management Setup.
Press "Finish" button to close this wizard, or click the following link to open other pages.
Return to Wizard Main Page
Go to Advanced Setup page
<Back
Finish

PART III
Advanced

Status Screens (117)
WAN Setup (127)
LAN Setup (143)
Wireless LAN (155)
Network Address Translation (NAT) Screens (173)
Voice (185)
VoIP Trunking (221)
Phone Usage (237)
Firewalls (241)
Content Filtering (261)
Introduction to IPSec (265)
VPN Screens (271)
Certificates (297)
Static Route (321)
Bandwidth Management (325)
Dynamic DNS Setup (333)
Remote Management Configuration (337)
Universal Plug-and-Play (UPnP) (347)

7

Status Screens

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts. The **Status** screen also provides detailed information from Any IP and DHCP and statistics from VoIP, bandwidth management, and traffic.

7.1 Status Screen

Click **Status** to open this screen.

Figure 88 Status Screen

Each field is described in the following table.

Table 17 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **Maintenance > System > General** screen's **System Name** field.
Model Number	This is the model name of your device.

Table 17 Status Screen

LABEL	DESCRIPTION
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
DSL Mode	This is the DSL standard that your ZyXEL Device is using.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or **WAN** screen.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
WLAN Information	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN. Click this to go to the screen where you can change it.
Channel	This is the channel number used by the ZyXEL Device now.
Security	This displays the type of security mode the ZyXEL Device is using in the wireless LAN.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated. Click this to go to the screen where you can change it.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated. Click this to go to the screen where you can change it.
System Status	
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it (see Section 1.6 on page 49).

Table 17 Status Screen

LABEL	DESCRIPTION
Current Date/ Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management; see Chapter 21 on page 325).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 29.6 on page 415, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface. For the WLAN interface, it displays **Active** when WLAN is enabled or **Inactive** when WLAN is disabled.
Rate	For the LAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
Summary	
Client List	Click this link to view current DHCP client information. See Section 9.6 on page 151.
AnyIP Table	Click this link to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device. See Section 7.2 on page 121.
WLAN Status	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See Section 7.3 on page 122.
Bandwidth Status	Click this link to view the ZyXEL Device's bandwidth usage and allotments. See Section 21.8 on page 332.
VPN Status	Click this link to view the ZyXEL Device's current VPN connections. See Section 18.16 on page 291.
Packet Statistics	Click this link to view port status and packet specific statistics. See Section 7.4 on page 122.
VoIP Statistics	Click this link to view statistics about your VoIP usage. See Section 7.5 on page 124.
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

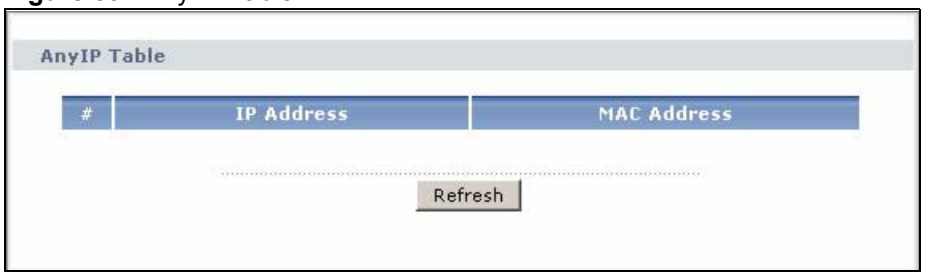
Table 17 Status Screen

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, • Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. • The second field displays **Registered**. If the SIP account is not registered with the SIP server, • Click **Register** to have the ZyXEL Device attempt to register the SIP account with the SIP server. • The second field displays the reason the account is not registered. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.

7.2 Any IP Table

Click **Status > AnyIP Table** to access this screen. Use this screen to view the IP address and MAC address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.

Figure 89 Any IP Table



Each field is described in the following table.

Table 18 Any IP Table

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
MAC Address	This field displays the MAC address of the computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
Refresh	Click this to update this screen.

7.3 WLAN Status

Click **Status > WLAN Status** to access this screen. Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

Figure 90 WLAN Status

The following table describes the labels in this screen.

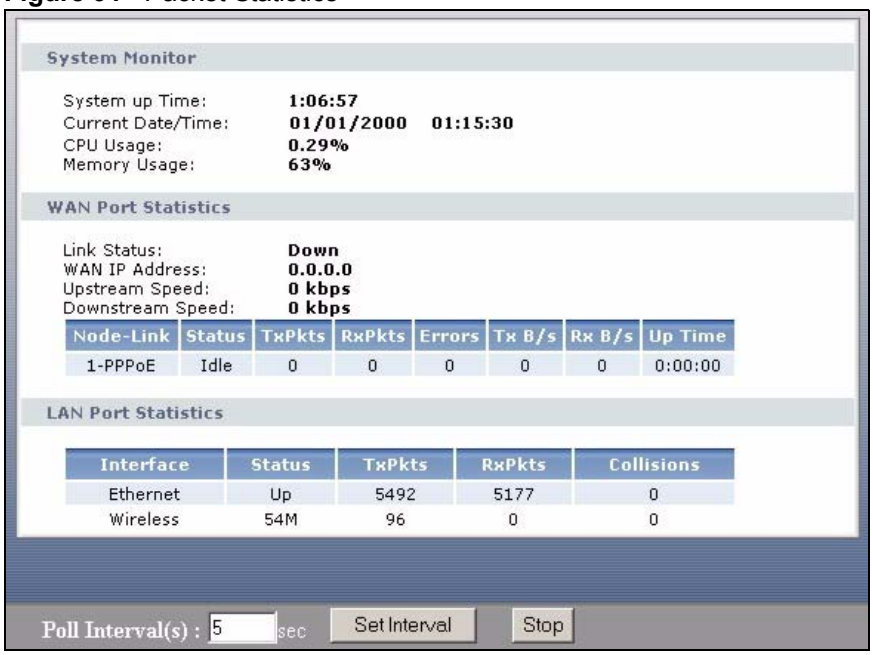
Table 19 WLAN Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station.
Association TIme	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click **Refresh** to reload this screen.

7.4 Packet Statistics

Click **Status > Packet Statistics** to access this screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 91 Packet Statistics


System Monitor
System up Time: 1:06:57
Current Date/Time: 01/01/2000 01:15:30
CPU Usage: 0.29%
Memory Usage: 63%
WAN Port Statistics
Link Status: Down
WAN IP Address: 0.0.0.0
Upstream Speed: 0 kbps
Downstream Speed: 0 kbps
Node-Link Status TxPkts RxPkts Errors Tx B/s Rx B/s Up Time
1-PPPoE Idle 0 0 0 0 0 0:00:00
LAN Port Statistics
Interface Status TxPkts RxPkts Collisions
Ethernet Up 5492 5177 0
Wireless 54M 96 0 0
Poll Interval(s) : 5 sec
Set Interval
Stop

The following table describes the fields in this screen.

Table 20 Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.
WAN IP Address	This is the IP address of the ZyXEL Device's WAN port.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
LAN Port Statistics	

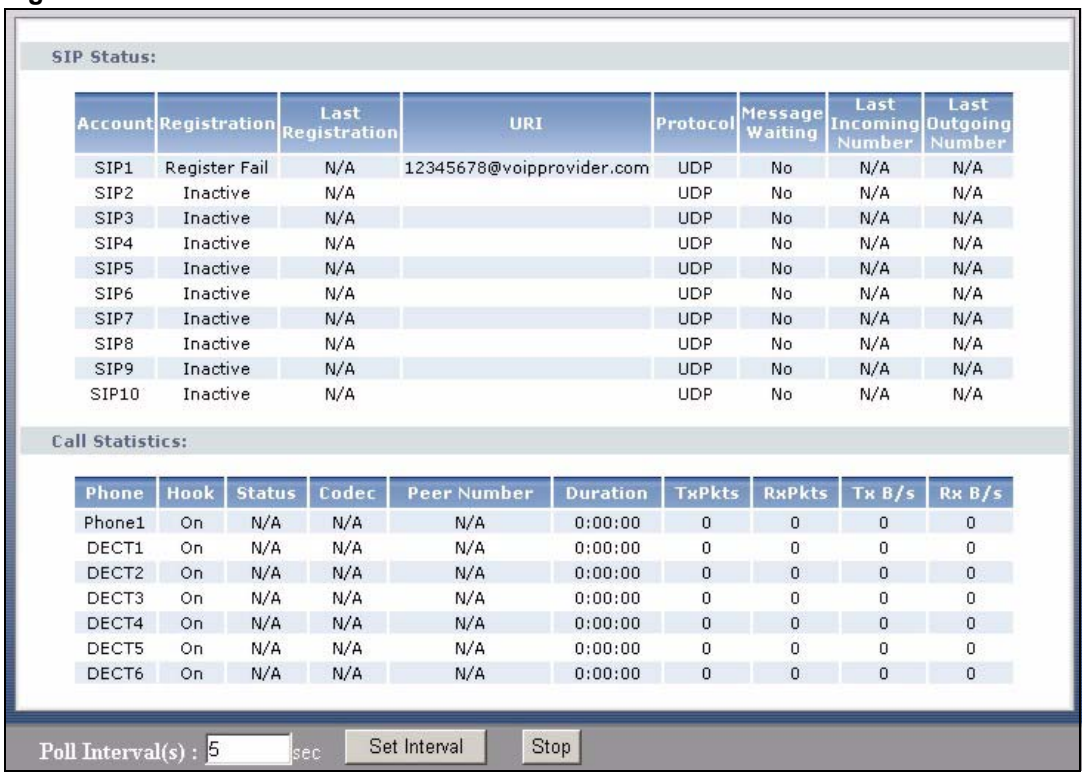
Table 20 Packet Statistics (continued)

LABEL	DESCRIPTION
Interface	This field displays either **Ethernet** (LAN ports) or **Wireless** (WLAN port).
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN port, it displays the transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This is the number of collisions on this interfaces.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

7.5 VoIP Statistics

Click **Status > VoIP Statistics** to access this screen.

Figure 92 VoIP Statistics


SIP Status:
Account Registration Last Registration URI Protocol Message Waiting Last Incoming Number Last Outgoing Number
SIP1 Register Fail N/A 12345678@voipprovider.com UDP No N/A N/A
SIP2 Inactive N/A UDP No N/A N/A
SIP3 Inactive N/A UDP No N/A N/A
SIP4 Inactive N/A UDP No N/A N/A
SIP5 Inactive N/A UDP No N/A N/A
SIP6 Inactive N/A UDP No N/A N/A
SIP7 Inactive N/A UDP No N/A N/A
SIP8 Inactive N/A UDP No N/A N/A
SIP9 Inactive N/A UDP No N/A N/A
SIP10 Inactive N/A UDP No N/A N/A
Call Statistics:
Phone Hook Status Codec Peer Number Duration TxPkts RxPkts Tx B/s Rx B/s
Phone1 On N/A N/A N/A 0:00:00 0 0 0 0
DECT1 On N/A N/A N/A 0:00:00 0 0 0 0
DECT2 On N/A N/A N/A 0:00:00 0 0 0 0
DECT3 On N/A N/A N/A 0:00:00 0 0 0 0
DECT4 On N/A N/A N/A 0:00:00 0 0 0 0
DECT5 On N/A N/A N/A 0:00:00 0 0 0 0
DECT6 On N/A N/A N/A 0:00:00 0 0 0 0
Poll Interval(s) : 5 sec
Set Interval
Stop

Each field is described in the following table.

Table 21 VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**.
Last Registration	This field displays the last time you successfully registered the SIP account. It displays **N/A** if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays **N/A** if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays **N/A** if the SIP account has never dialed a number.
Call Statistics	
Phone	This field displays each phone port or DECT port in the ZyXEL Device.
Hook	This field indicates whether the phone is on the hook or off the hook. **On** - The phone is hanging up or already hung up. **Off** - The phone is dialing, calling, or connected.
Status	This field displays the current state of the phone call. **N/A** - There are no current VoIP calls, incoming calls or outgoing calls being made. **DIAL** - The callee's phone is ringing. **RING** - The phone is ringing for an incoming VoIP call. **Process** - There is a VoIP call in progress. **DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Duration	This field displays how long the current call has lasted.
Tx Pkts	This field displays the number of packets the ZyXEL Device has transmitted in the current call.
Rx Pkts	This field displays the number of packets the ZyXEL Device has received in the current call.
Tx B/s	This field displays how quickly the ZyXEL Device has transmitted packets in the current call. The rate is the average number of bytes transmitted per second.

Table 21 VoIP Statistics

LABEL	DESCRIPTION
Rx B/s	This field displays how quickly the ZyXEL Device has received packets in the current call. The rate is the average number of bytes transmitted per second.
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click **Set Interval**.
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in **Poll Interval**.
Stop	Click this to make the ZyXEL Device stop updating the screen.

8

WAN Setup

This chapter describes how to configure WAN settings.

8.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

8.1.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

8.1.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Gateway IP Address** field in the wizard or WAN screen. You can get this information from your ISP.

8.1.1.2 PPP over Ethernet

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

8.1.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

8.1.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

8.1.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

8.1.2.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

8.1.2.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

8.1.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

8.1.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

8.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the **IP Address** field and *not* the **Gateway IP Address** field.

8.1.4.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment *must* be static.

8.1.4.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **Gateway IP Address** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN port and so the **IP Address** and **Gateway IP Address** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

8.1.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

8.1.6 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.2 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL Device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL Device uses the following pre-defined priorities:

- Normal route: designated by the ISP (see Section 8.5 on page 131)
- Traffic-redirect route (see Section 8.7 on page 140)

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL Device tries the traffic-redirect route next.

8.3 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

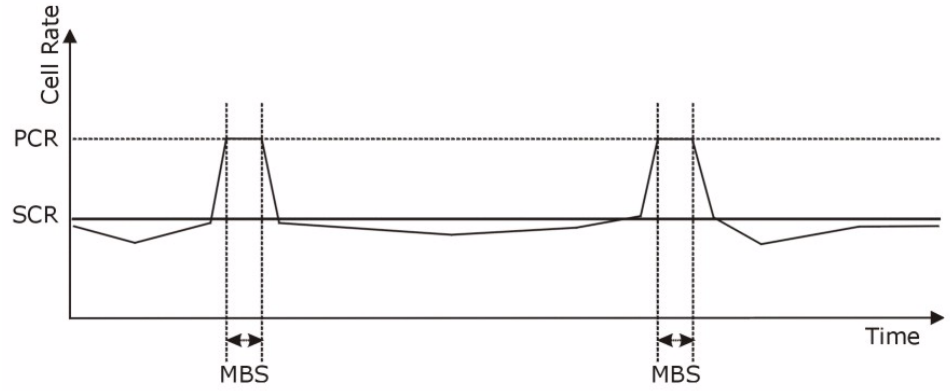
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 93 Example of Traffic Shaping



8.3.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

8.3.1.1 Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

8.3.1.2 Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

8.3.1.3 Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

8.4 Zero Configuration Internet Access

Once you turn on and connect the ZyXEL Device to a telephone jack, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

Zero configuration for Internet access is disabled when

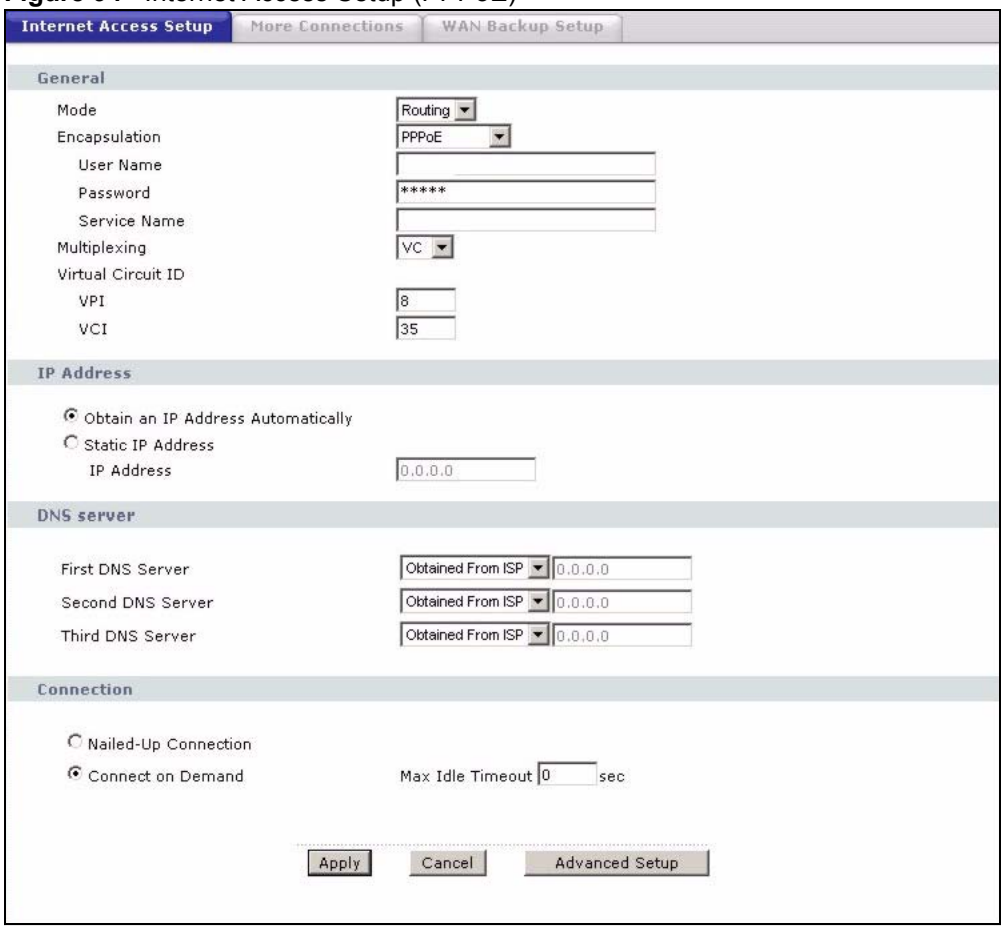
- the ZyXEL Device is in bridge mode
- you set the ZyXEL Device to use a static (fixed) WAN IP address.

8.5 Internet Access Setup

Use this screen to change your ZyXEL Device’s WAN remote node settings. Click **Network > WAN > Internet Access Setup**. The screen differs by the encapsulation you select.

See Section 8.1 on page 127 for more information.

Figure 94 Internet Access Setup (PPPoE)



The following table describes the labels in this screen.

Table 22 Internet Access Setup

LABEL	DESCRIPTION
General	
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account. Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the ZyXEL Device.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.

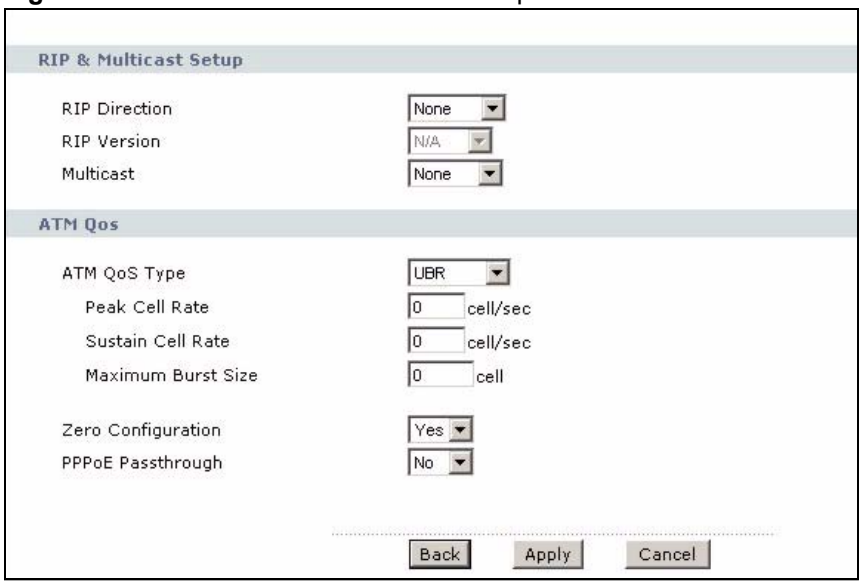
Table 22 Internet Access Setup (continued)

LABEL	DESCRIPTION
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation.
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select **ENET ENCAP** in the **Encapsulation** field
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address) and you select **Obtain an IP Address Automatically**. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **Advanced WAN Setup** screen and edit more details of your WAN setup.

8.5.1 Advanced Internet Access Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

Figure 95 Advanced Internet Access Setup



The following table describes the labels in this screen.

Table 23 Advanced Internet Access Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	This field is not configurable if you select **None** in the **RIP Direction** field. Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-RT** (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select **VBR-nRT** (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.

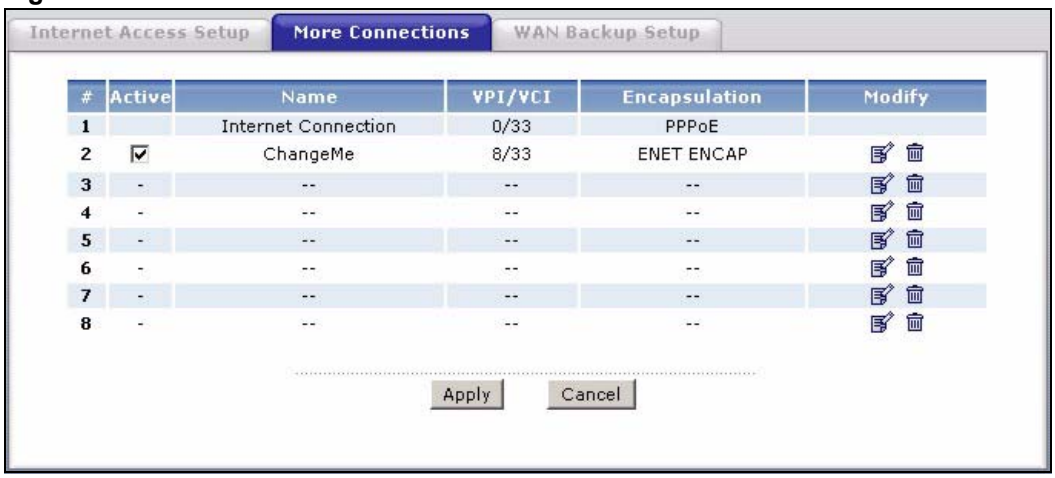
Table 23 Advanced Internet Access Setup (continued)

LABEL	DESCRIPTION
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select **Yes** to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select **No** to disable this feature. You must manually configure the ZyXEL Device for Internet access.
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select **PPPoE** encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.6 WAN More Connections

The ZyXEL Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation you select. When you use the **WAN > Internet Access Setup** screen to set up Internet access, you are configuring the first WAN connection.

Figure 96 WAN More Connections


Internet Access Setup
More Connections
WAN Backup Setup
Active Name VPI/VCI Encapsulation Modify
1 Internet Connection 0/33 PPPoE
2 ChangeMe 8/33 ENET ENCAP
3 - -- -- --
4 - -- -- --
5 - -- -- --
6 - -- -- --
7 - -- -- --
8 - -- -- --
Apply
Cancel

The following table describes the labels in this screen.

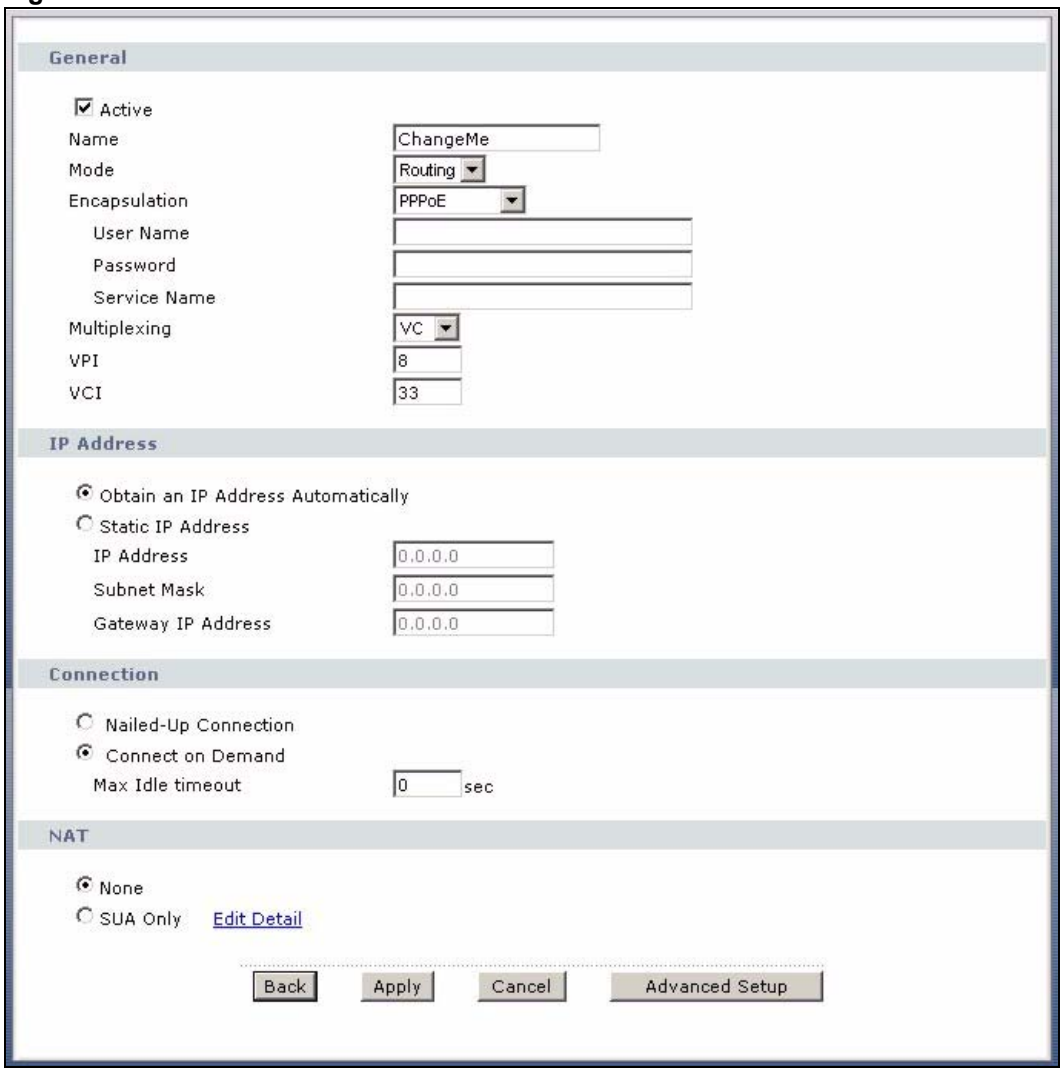
Table 24 Advanced Internet Access Setup

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not. Clear the check box to disable the connection. Select the check box to enable it.
Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the **WAN > Internet Access Setup** screen to edit it. Click the Edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the Remove icon to delete the Internet access setup from your connection list.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.6.1 More Connections Edit

Click the edit icon in the **More Connections** screen to configure a connection.

Figure 97 More Connections Edit



The following table describes the labels in this screen.

Table 25 More Connections Edit

LABEL	DESCRIPTION
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.
Mode	Select **Routing** from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select **Bridge**, the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.

Table 25 More Connections Edit (continued)

LABEL	DESCRIPTION
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol. For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. If you use the encapsulation type except **RFC 1483**, select **Obtain an IP Address Automatically** when you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below. If you use **RFC 1483**, enter the IP address given by your ISP in the **IP Address** field.
Subnet Mask	Enter a subnet mask in dotted decimal notation.
Gateway IP address	Specify a gateway IP address (supplied by your ISP).
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
NAT	**SUA only** is available only when you select **Routing** in the **Mode** field. Select **SUA Only** if you have one public IP address and want to use NAT. Click **Edit** to go to the **Port Forwarding** screen to edit a server mapping set. Otherwise, select **None** to disable NAT.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.

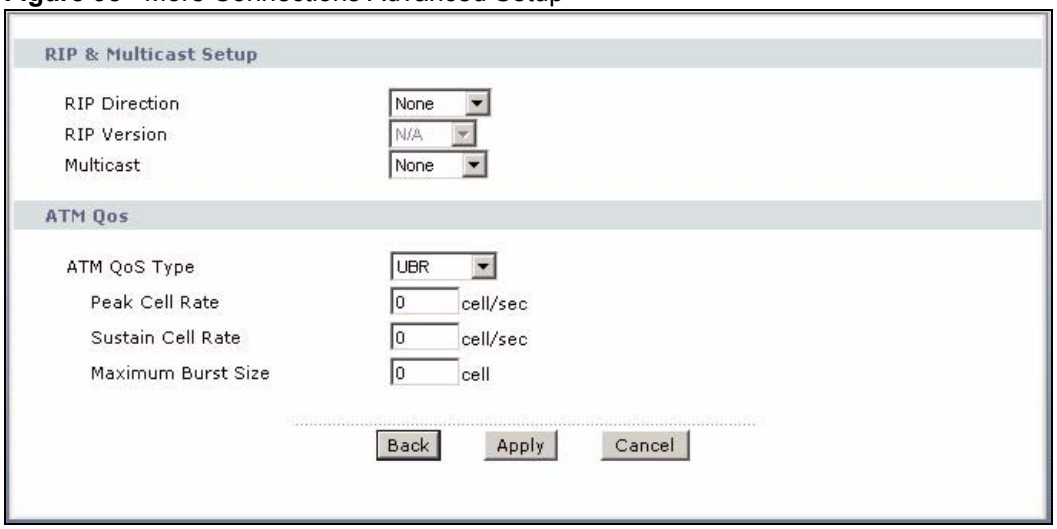
Table 25 More Connections Edit (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **More Connections Advanced Setup** screen and edit more details of your WAN setup.

8.6.2 Configuring More Connections Advanced Setup

To edit your ZyXEL Device's advanced WAN settings, click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

Figure 98 More Connections Advanced Setup



The following table describes the labels in this screen.

Table 26 More Connections Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-nRT** (Variable Bit Rate-non Real Time) or **VBR-RT** (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.

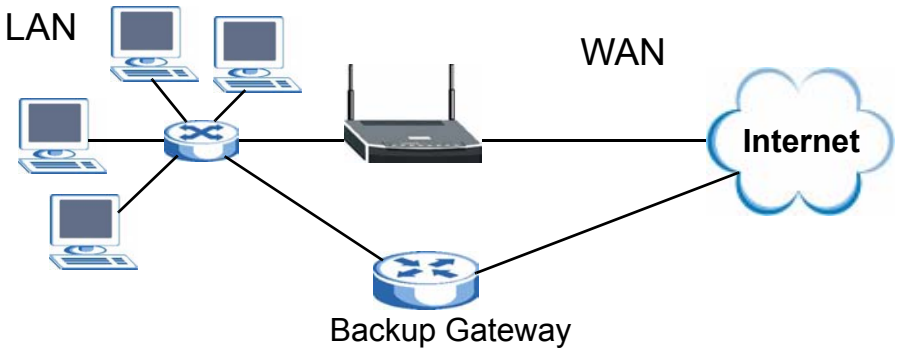
Table 26 More Connections Advanced Setup (continued)

LABEL	DESCRIPTION
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.7 Traffic Redirect

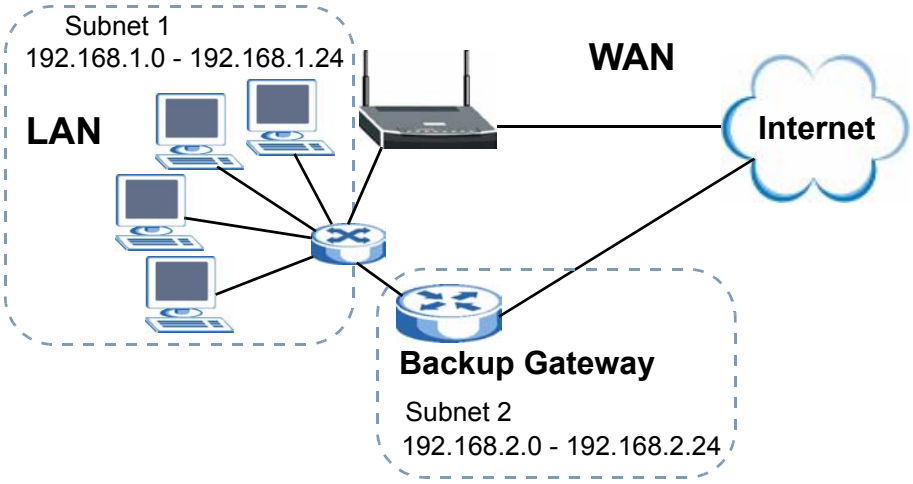
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

Figure 99 Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the ZyXEL Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

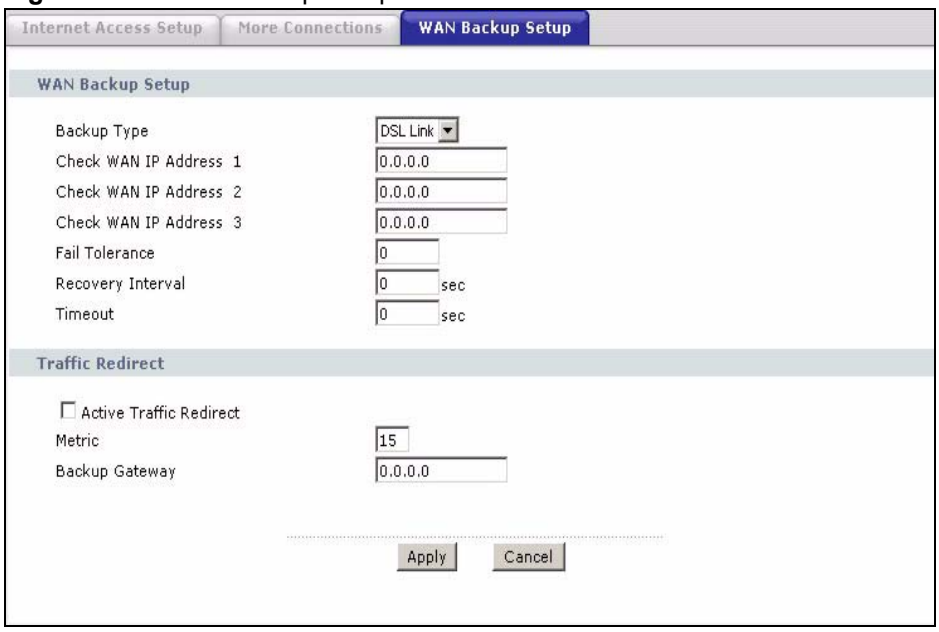
Figure 100 Traffic Redirect LAN Setup



8.8 WAN Backup Setup

Use this screen to configure your ZyXEL Device's WAN backup. Click **Network > WAN > WAN Backup Setup**.

Figure 101 WAN Backup Setup



The following table describes the labels in this screen.

Table 27 WAN Backup Setup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select **DSL Link** to have the ZyXEL Device check if the connection to the DSLAM is up. Select **ICMP** to have the ZyXEL Device periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.

Table 27 WAN Backup Setup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9

LAN Setup

This chapter describes how to configure LAN settings.

9.1 LAN Overview

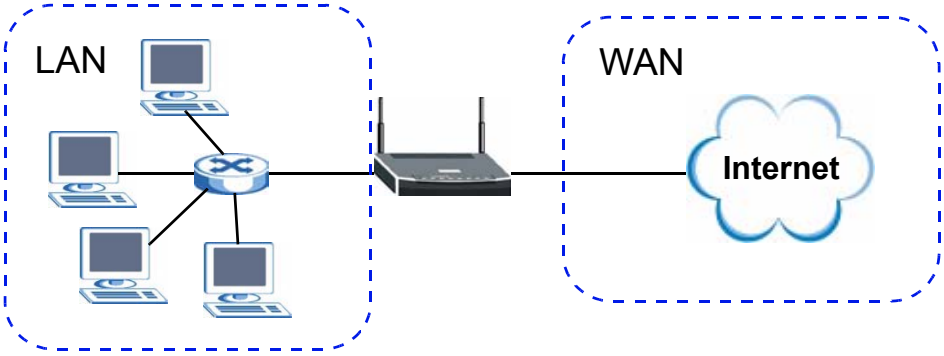
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See Section 9.4 on page 148 to configure the **LAN** screens.

9.1.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 102 LAN and WAN IP Addresses



9.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

9.1.2.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

9.2 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

  If the **DNS Server** fields in the **DHCP Setup** screen are set to **DNS Relay**, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

9.3 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

9.3.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

9.3.1.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

9.3.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

9.3.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

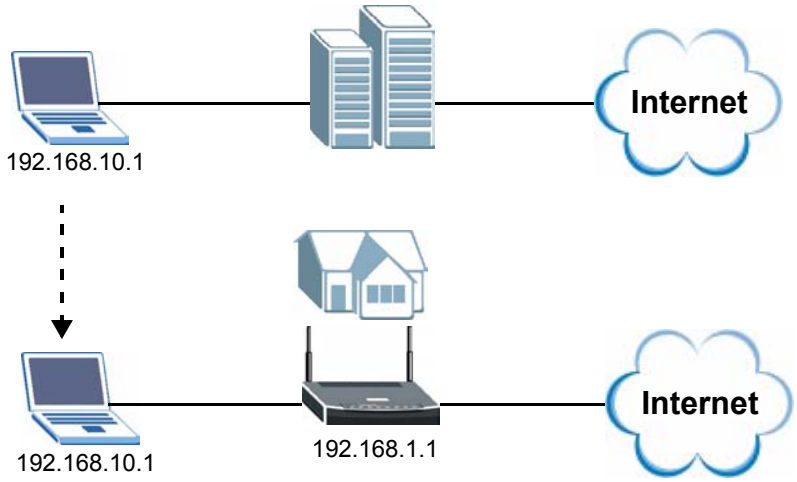
9.3.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the ZyXEL Device to be in the same subnet to allow the computer to access the Internet (through the ZyXEL Device). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the ZyXEL Device.

With the Any IP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a ZyXEL Device is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

Figure 103 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyXEL Device's IP address.

You must enable NAT/SUA to use the Any IP feature on the ZyXEL Device.

9.3.4.1 How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the ZyXEL Device) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the ZyXEL Device.

1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.

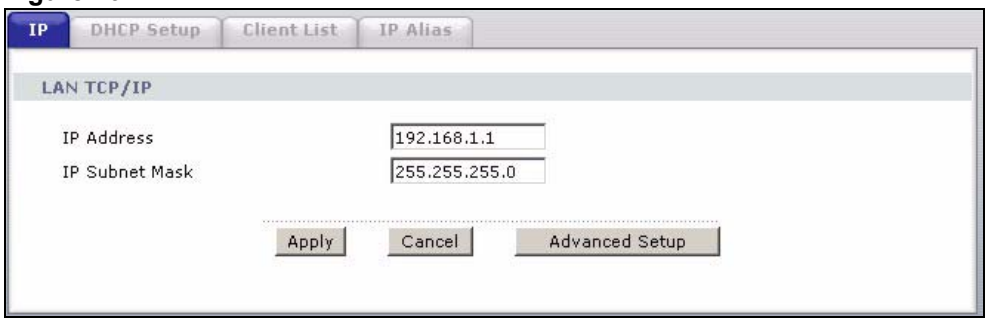
3 The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.
4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.
5 When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the ZyXEL Device and the Internet as if it is in the same subnet as the ZyXEL Device.

9.4 Configuring LAN IP

Click **Network > LAN** to open the **IP** screen. See Section 9.1 on page 143 for background information. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device.

Figure 104 LAN IP



The following table describes the fields in this screen.

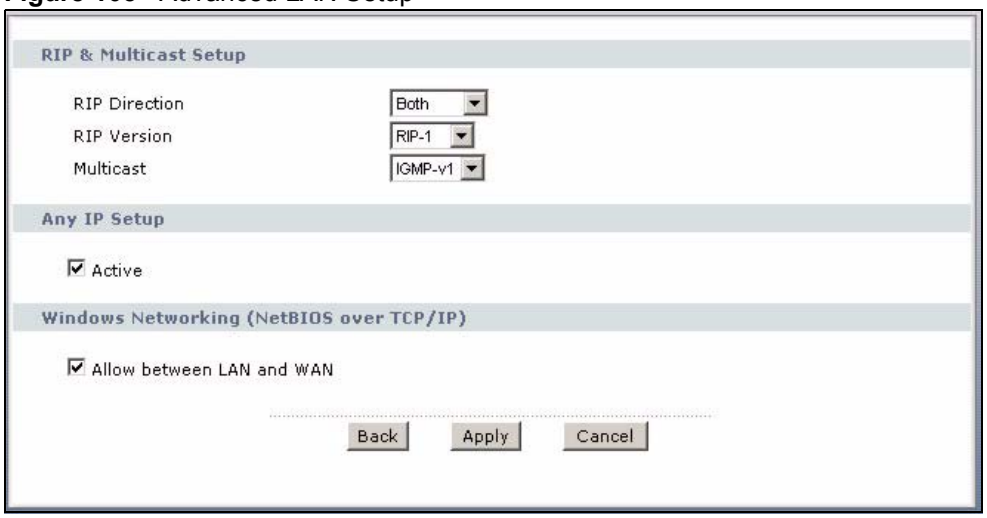
Table 28 LAN IP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **Advanced LAN Setup** screen and edit more details of your LAN setup.

9.4.1 Configuring Advanced LAN Setup

Use this screen to edit your ZyXEL Device's RIP, multicast, any IP and Windows Networking settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

Figure 105 Advanced LAN Setup



The following table describes the labels in this screen.

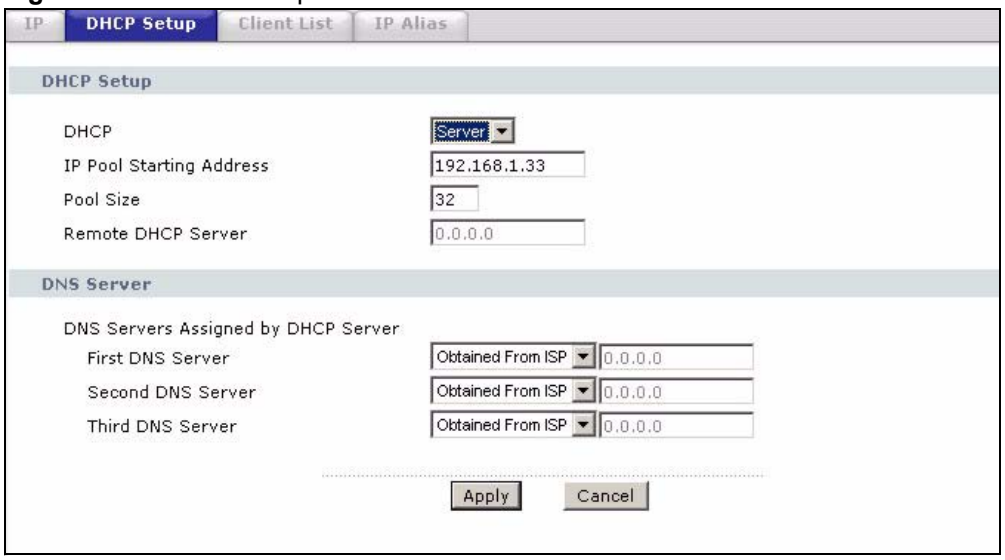
Table 29 Advanced LAN Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Any IP Setup	Select the **Active** check box to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5 DHCP Setup

Click **Network > DHCP Setup** to open this screen. Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 106 DHCP Setup



The following table describes the labels in this screen.

Table 30 DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	If set to **Server**, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.

Table 30 DHCP Setup

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyXEL Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select `None` if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

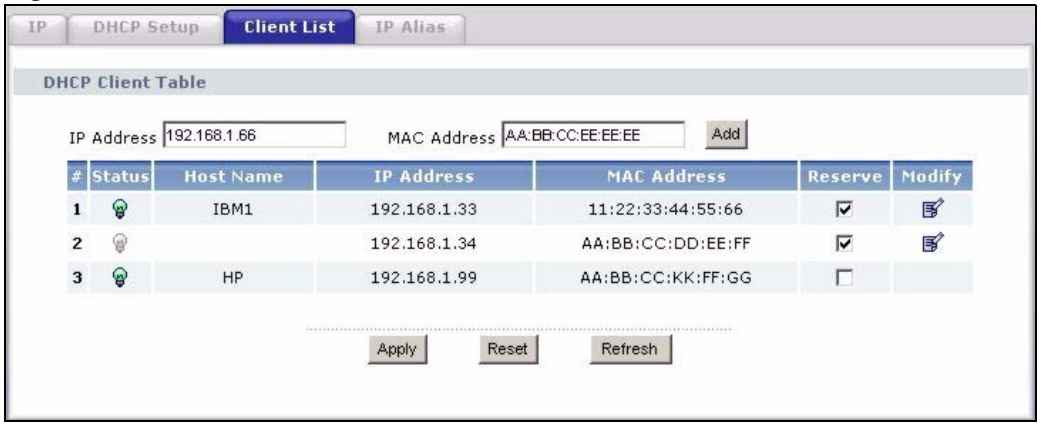
9.6 LAN Client List

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Click **Network > LAN > Client List** to open the following screen. Use this screen to change your ZyXEL Device's static DHCP settings.

Figure 107 LAN Client List



The following table describes the labels in this screen.

Table 31 LAN Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click **Add** to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to reload the DHCP table.

9.7 LAN IP Alias

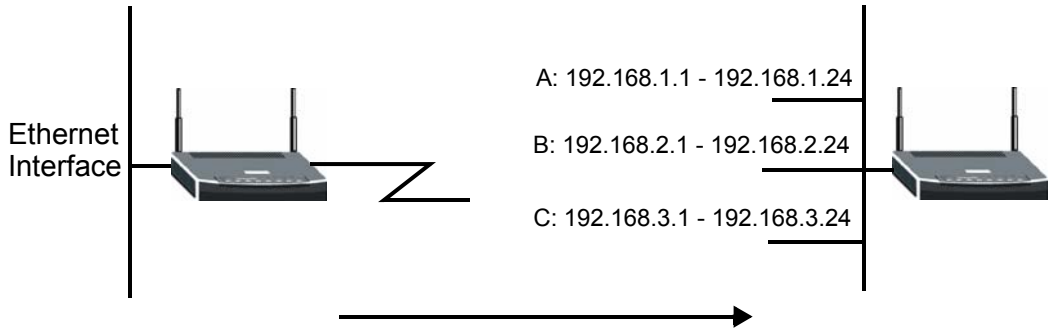
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Make sure that the subnets of the logical networks do not overlap.

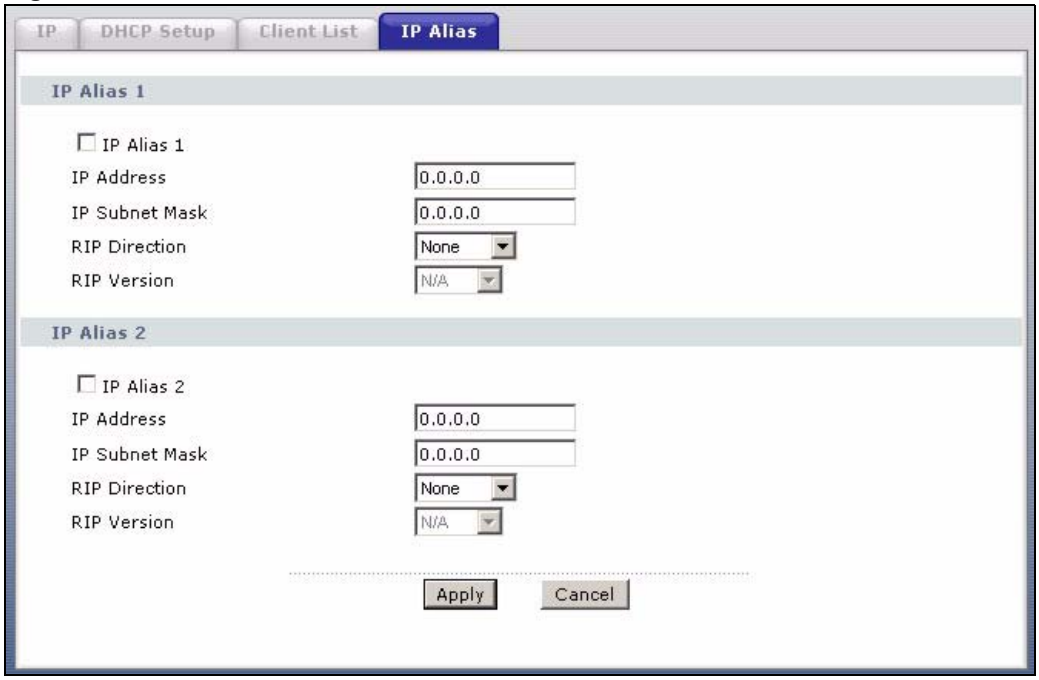
The following figure shows a LAN divided into subnets A, B, and C.

Figure 108 Physical Network & Partitioned Logical Networks



Click **Network** > **LAN** > **IP Alias** to open the following screen. Use this screen to change your ZyXEL Device's IP alias settings.

Figure 109 LAN IP Alias



The following table describes the labels in this screen.

Table 32 LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.

Table 32 LAN IP Alias

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both/In Only/Out Only/None**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10

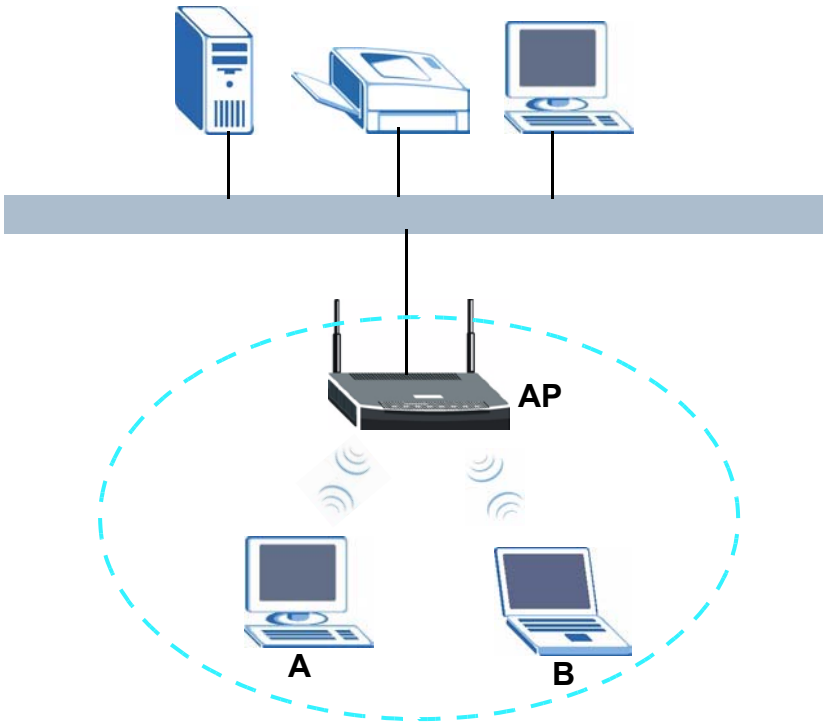
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks. This chapter applies to the "W" models only.

10.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 110 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use a different channel.
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

10.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

10.2.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

10.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

10.2.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

10.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 10.2.3 on page 156 for information about this.)

Table 33 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

10.2.5 One-Touch Intelligent Security Technology (OTIST)

With ZyXEL's OTIST, you set up the SSID and the encryption (WEP or WPA-PSK) on the ZyXEL Device. Then, the ZyXEL Device transfers them to the devices in the wireless networks. As a result, you do not have to set up the SSID and encryption on every device in the wireless network.

The devices in the wireless network have to support OTIST, and they have to be in range of the ZyXEL Device when you activate it. See Section 10.6 on page 165 for more details.

10.3 Wireless Performance Overview

The following sections introduce different ways to improve the performance of the wireless network.

10.3.1 Quality of Service (QoS)

You can turn on Wi-Fi MultiMedia (WMM) QoS to improve the performance of voice and video applications in the wireless network. QoS gives high priority to voice and video, which makes them run more smoothly. Similarly, it gives low priority to many large file downloads so that they do not reduce the quality of other applications.

10.4 Additional Wireless Terms

The following table describes wireless network terms and acronyms used in the ZyXEL Device's Web Configurator.

Table 34 Additional Wireless Terms

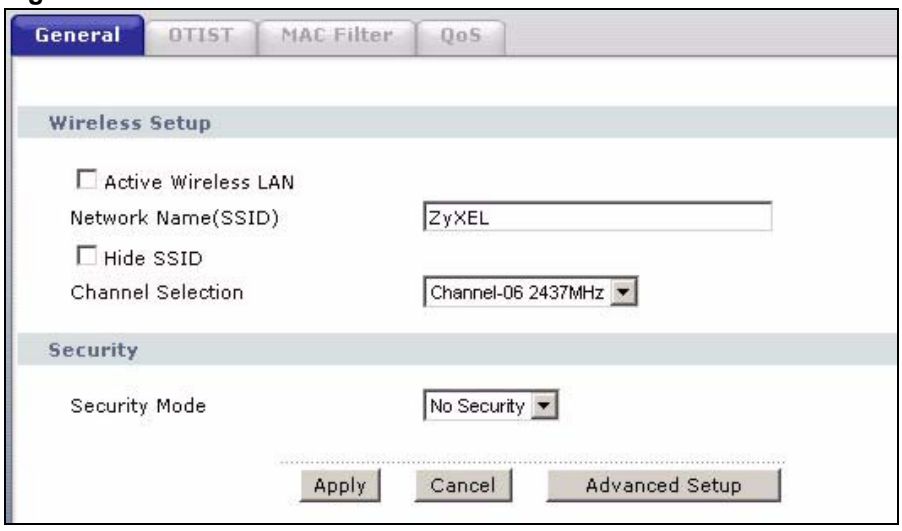
TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

10.5 General WLAN Screen

If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **Wireless LAN General** screen.

Figure 111 Wireless LAN: General



The following table describes the labels in this screen.

Table 35 Wireless LAN: General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

Table 35 Wireless LAN: General

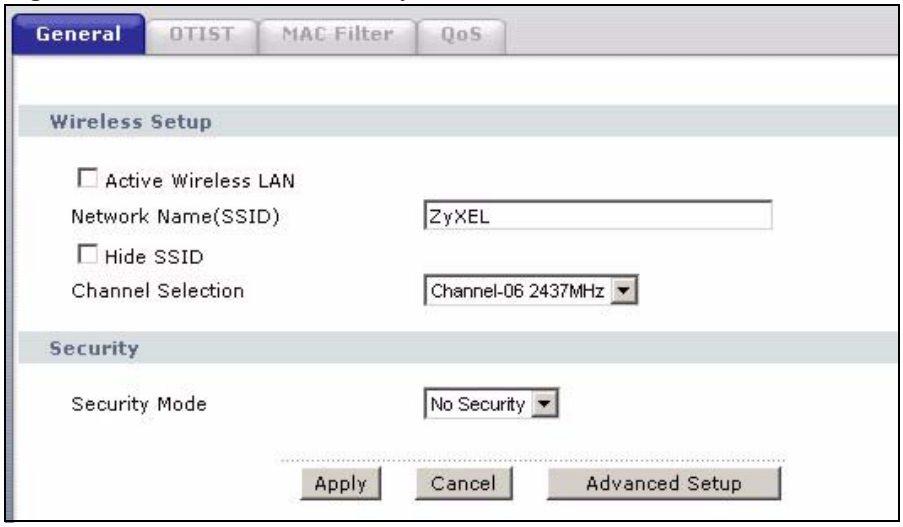
LABEL	DESCRIPTION
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Security Mode	See the following sections for more details about this field.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Advanced Setup	Click **Advanced Setup** to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup.

10.5.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Figure 112 Wireless: No Security



The following table describes the labels in this screen.

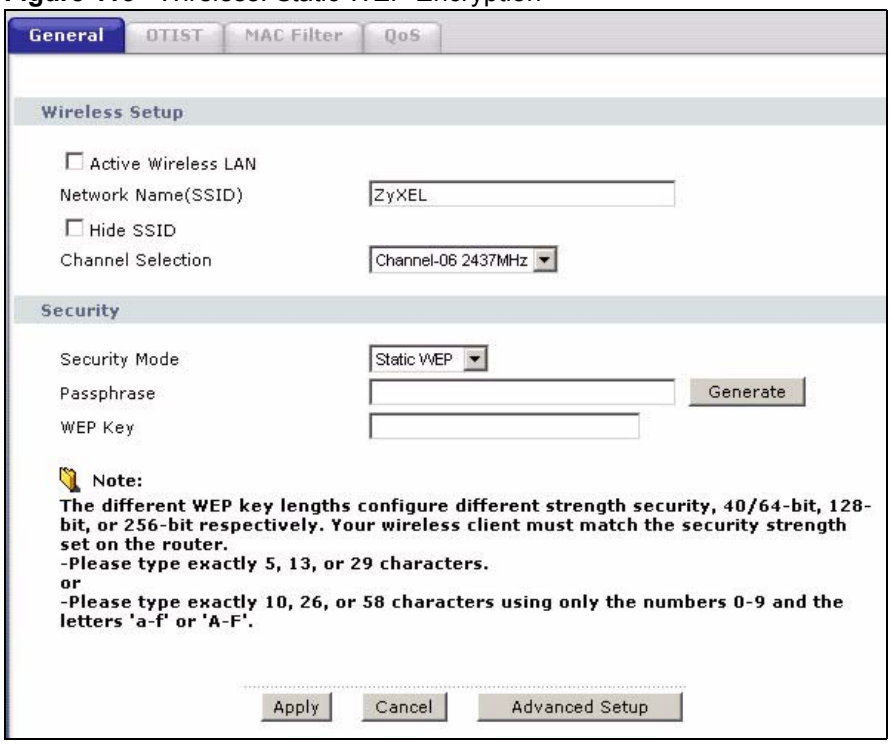
Table 36 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.

10.5.2 WEP Encryption Screen

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 113 Wireless: Static WEP Encryption



The following table describes the wireless LAN security labels in this screen.

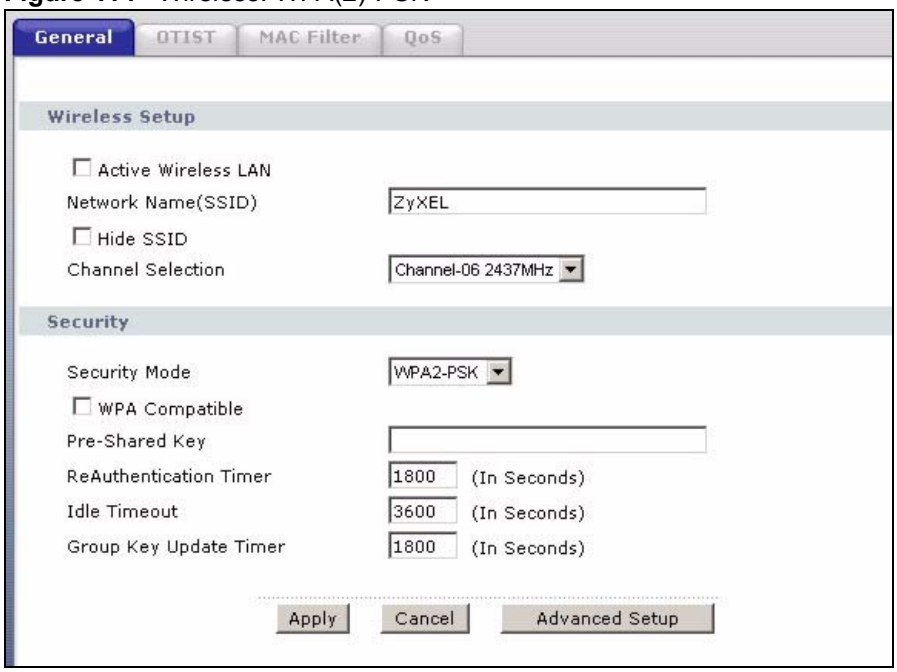
Table 37 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** from the drop-down list box.
Passphrase	Enter a passphrase (up to 32 printable characters) and clicking **Generate**. The ZyXEL Device automatically generates a WEP key.
WEP Key	The WEP key is used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.

10.5.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 114 Wireless: WPA(2)-PSK



The following table describes the wireless LAN security labels in this screen.

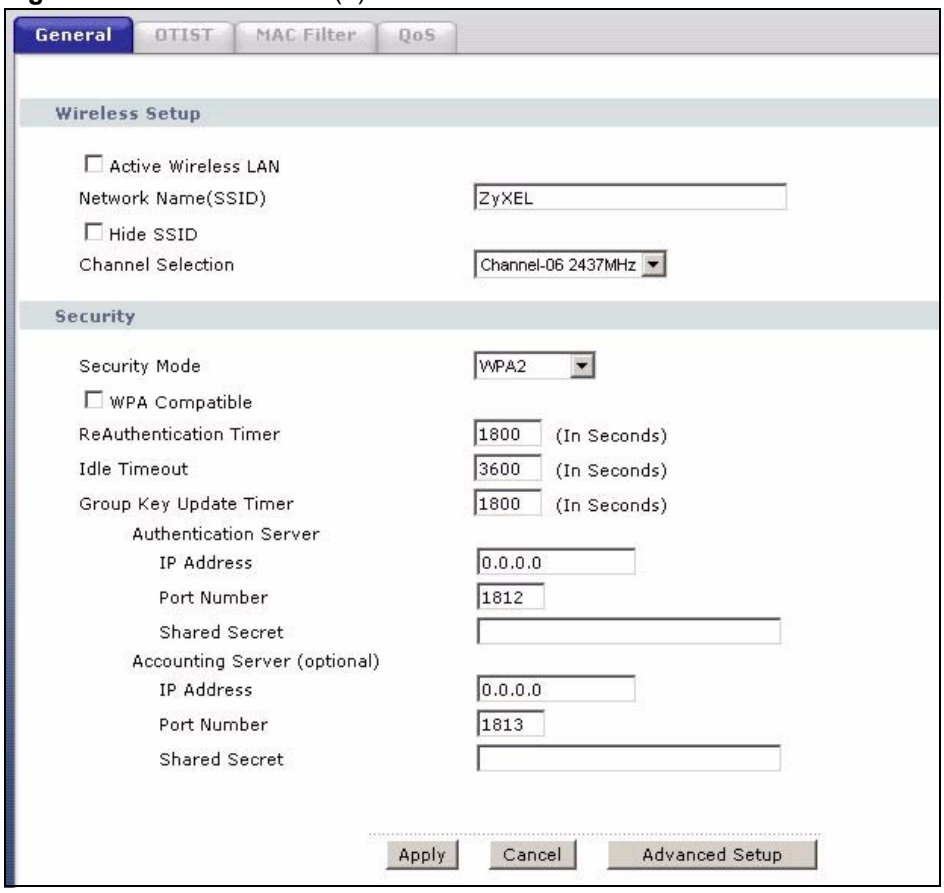
Table 38 Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
WPA Compatible	This field is only available for WPA2-PSK. Select this if you want the ZyXEL Device to support WPA-PSK and WPA2-PSK simultaneously.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPAWPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. The ZyXEL Device default is **1800** seconds (30 minutes).

10.5.4 WPA(2) Authentication Screen

In order to configure and enable WPA Authentication; click the **Wireless LAN** link under **Network** to display the **Wireless** screen. Select **WPA** or **WPA2** from the **Security** list.

Figure 115 Wireless: WPA(2)



The following table describes the wireless LAN security labels in this screen.

Table 39 Wireless: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

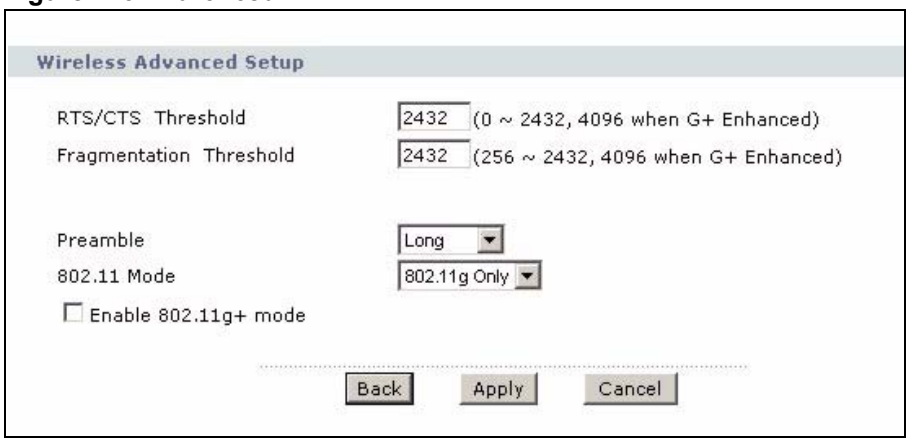
Table 39 Wireless: WPA(2)

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. The ZyXEL Device default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server (optional)	
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.

10.5.5 Wireless LAN Advanced Setup

To configure advanced wireless settings, click the **Advanced Setup** button in the **General** screen. The screen appears as shown.

Figure 116 Advanced



The following table describes the labels in this screen.

Table 40 Wireless LAN: Advanced

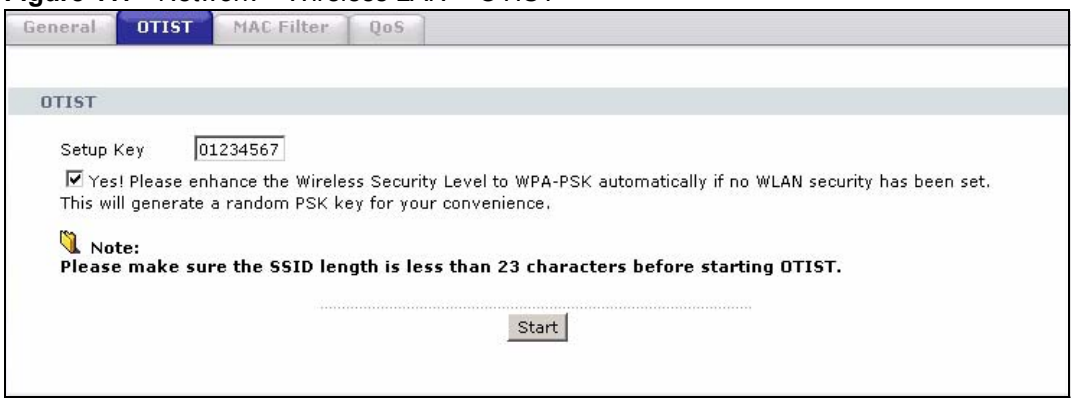
LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the **Enable 802.11g+ mode** checkbox a value of 4096 is displayed.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the **Enable 802.11g+ mode** checkbox a value of 4096 is displayed.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the appendix for more information.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Enable 802.11g+ mode	Select **Enable 802.11g+ mode** checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the ZyXEL Device at higher transmission speeds. This permits the ZyXEL Device to transmit at a higher speed than the **802.11g Only** mode.
Back	Click this to return to the previous screen without saving changes.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.6 OTIST Screen

Use this screen to set up and start OTIST on the ZyXEL Device in your wireless network. To open this screen, click **Network > Wireless LAN > OTIST**.

Ensure that your network's SSID is fewer than 23 characters in length before you start OTIST. Click **WIRELESS > General** to change your network's SSID.

Figure 117 Network > Wireless LAN > OTIST


General
OTIST
MAC Filter
QoS
OTIST
Setup Key
01234567
Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set.
This will generate a random PSK key for your convenience.
Note:
Please make sure the SSID length is less than 23 characters before starting OTIST.
Start

The following table describes the labels in this screen.

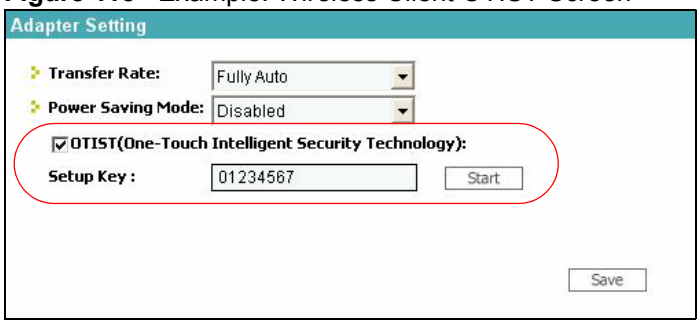
Table 41 Network > Wireless LAN > OTIST

LABEL	DESCRIPTION
Setup Key	Type a key (password) 8 ASCII characters long. Note: If you change the OTIST setup key in the ZyXEL Device, you must change it on the wireless devices too.
Yes!	Select this if you want the ZyXEL Device to automatically generate a pre-shared key for the wireless network. Before you do this, click **Network > Wireless LAN > General** and set the **Security Mode** to **No Security**. Clear this if you want the ZyXEL Device to use a pre-shared key that you enter. Before you do this, click **Network > Wireless LAN > General**, set the **Security Mode** to **WPA-PSK**, and enter the **Pre-Shared Key**.
Start	Click **Start** to activate OTIST and transfer settings. The process takes three minutes to complete. Note: You must click **Start** in the ZyXEL Device and in the wireless device(s) within three minutes of each other. You can start OTIST in the wireless devices and the ZyXEL Device in any order.

Before you click **Start**, you should enable OTIST on all the OTIST-enabled devices in the wireless network. For most devices, follow these steps.

1. Start the ZyXEL utility
2. Click the **Adapter** tab.
3. Select the **OTIST** check box, and enter the same **Setup Key** as the ZyXEL Device.
4. Click **Save**.

Figure 118 Example: Wireless Client OTIST Screen

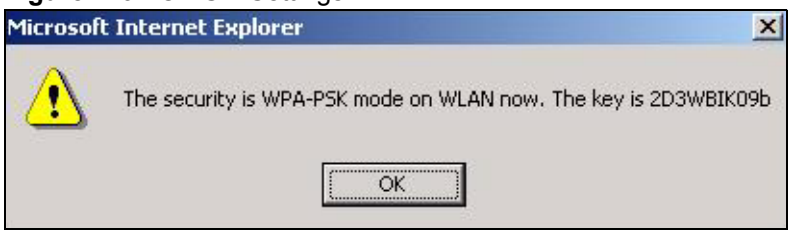


To start OTIST in the device, click **Start** in this screen.

You must click **Start** in the ZyXEL Device and in the wireless device(s) within three minutes of each other. You can start OTIST in the wireless devices and the ZyXEL Device in any order.

After you click **Start** in the ZyXEL Device, the following screen appears (in the ZyXEL Device).

Figure 119 OTIST: Settings



You can use the key in this screen to set up WPA-PSK encryption manually for non-OTIST devices in the wireless network.

Review the settings, and click **OK**. The ZyXEL Device begins transferring OTIST settings. The following screens appear in the ZyXEL Device and in the wireless devices.

Figure 120 OTIST: In Progress on the ZyXEL Device

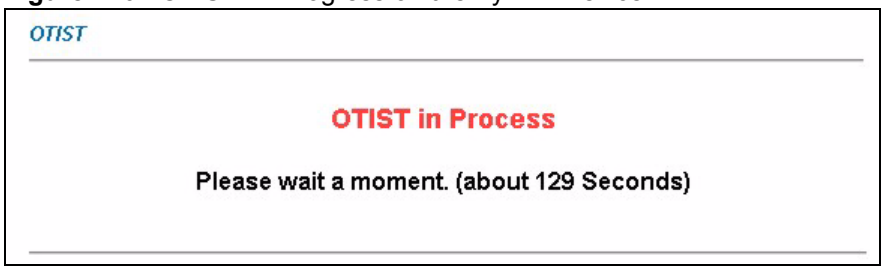
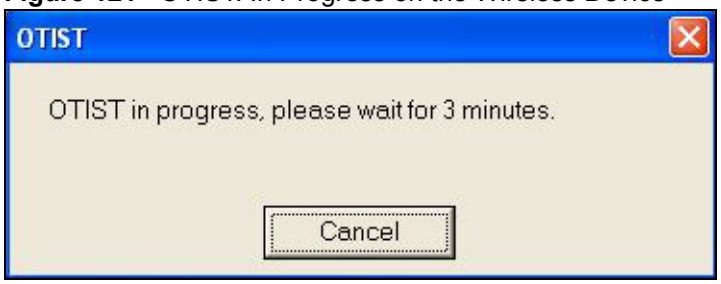


Figure 121 OTIST: In Progress on the Wireless Device



These screens close when the transfer is complete.

10.6.1 Notes on OTIST

1 If you enable OTIST in a wireless device, you see this screen each time you start the utility. Click **Yes** to search for an OTIST-enabled AP (in other words, the ZyXEL Device).

Figure 122 Start OTIST?

2 If an OTIST-enabled wireless device loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless device search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)

3 After the wireless device finds an OTIST-enabled AP, you must click **Start** in the ZyXEL Device's **Network > Wireless LAN > OTIST** screen or hold in the WLAN button on the ZyXEL Device for five seconds to transfer the settings again.

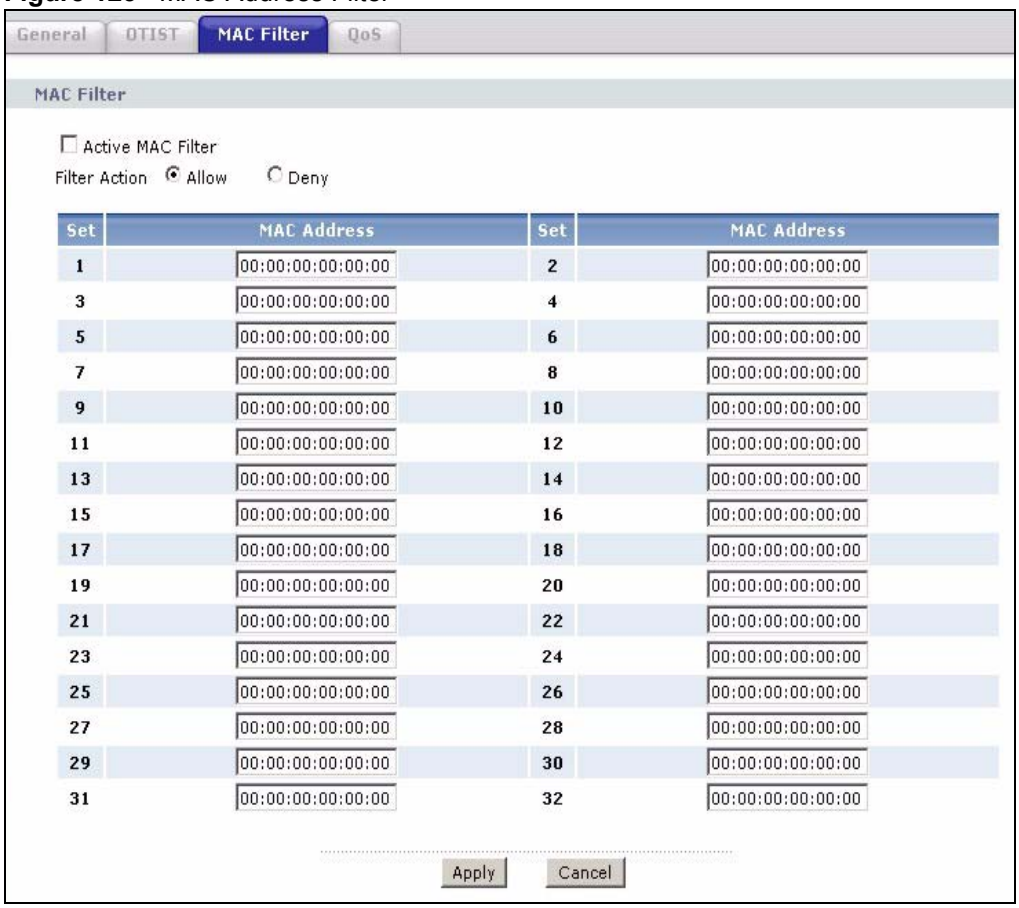
4 If you change the SSID or the keys on the ZyXEL Devices after using OTIST, you need to run OTIST again or enter them manually in the wireless device(s).

5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless device joins your wireless network, you need to run OTIST on the AP and ALL wireless devices again.

10.7 MAC Filter

Use this screen to change your ZyXEL Device's MAC filter settings. Click **Network > Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 123 MAC Address Filter



The following table describes the labels in this screen.

Table 42 MAC Address Filter

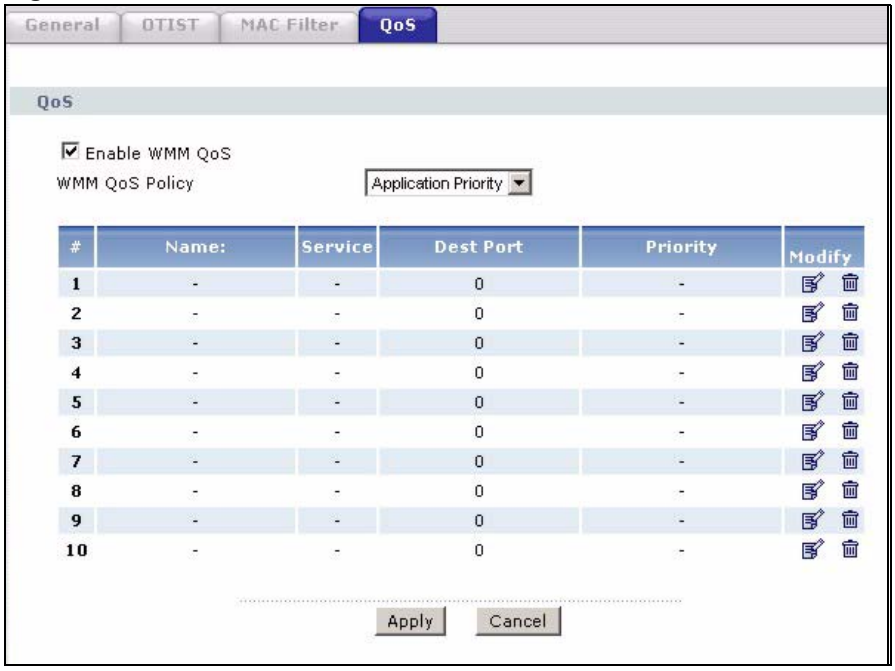
LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device Select **Allow** to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.8 QoS Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network > Wireless LAN** > **QoS**. The following screen displays.

Figure 124 Wireless LAN: QoS



The following table describes the fields in this screen.

Table 43 Wireless LAN: QoS

LABEL	DESCRIPTION
QoS Setup	
Enable WMM QoS	Select the check box to enable WMM QoS on the ZyXEL Device.
WMM QoS Policy	Select **Default** to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select **Application Priority** from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select **Application Priority** in **WMM QoS Policy**.
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either **FTP**, **WWW**, **E-mail** or a **User Defined** service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.

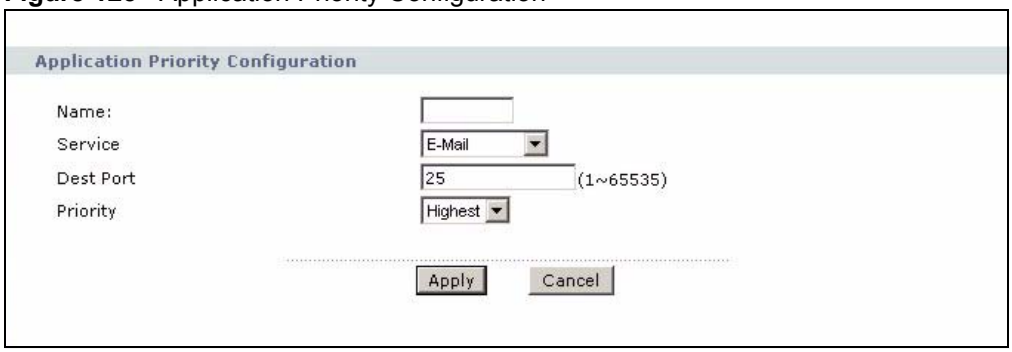
Table 43 Wireless LAN: QoS

LABEL	DESCRIPTION
Priority	This field displays the priority of the application. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Mid** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the **Edit** icon to open the **Application Priority Configuration** screen. Modify an existing application entry or create a application entry in the **Application Priority Configuration** screen. Click the **Remove** icon to delete an application entry.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

10.8.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

Figure 125 Application Priority Configuration



See Appendix E on page 499 for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

Table 44 Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.

Table 44 Application Priority Configuration

LABEL	DESCRIPTION
Service	The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box. • **E-Mail** Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • **FTP** File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21. • **WWW** The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. • **User defined** User-defined services are user specific services configured using known ports and applications.
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previous screen.

11

Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

11.1 NAT General Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

11.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 45 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

11.1.2 What NAT Does

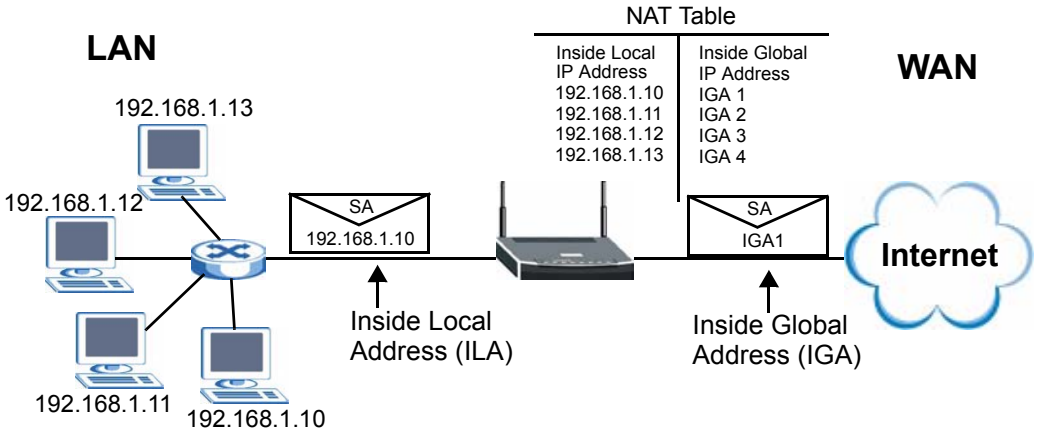
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see Table 46 on page 176), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

11.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

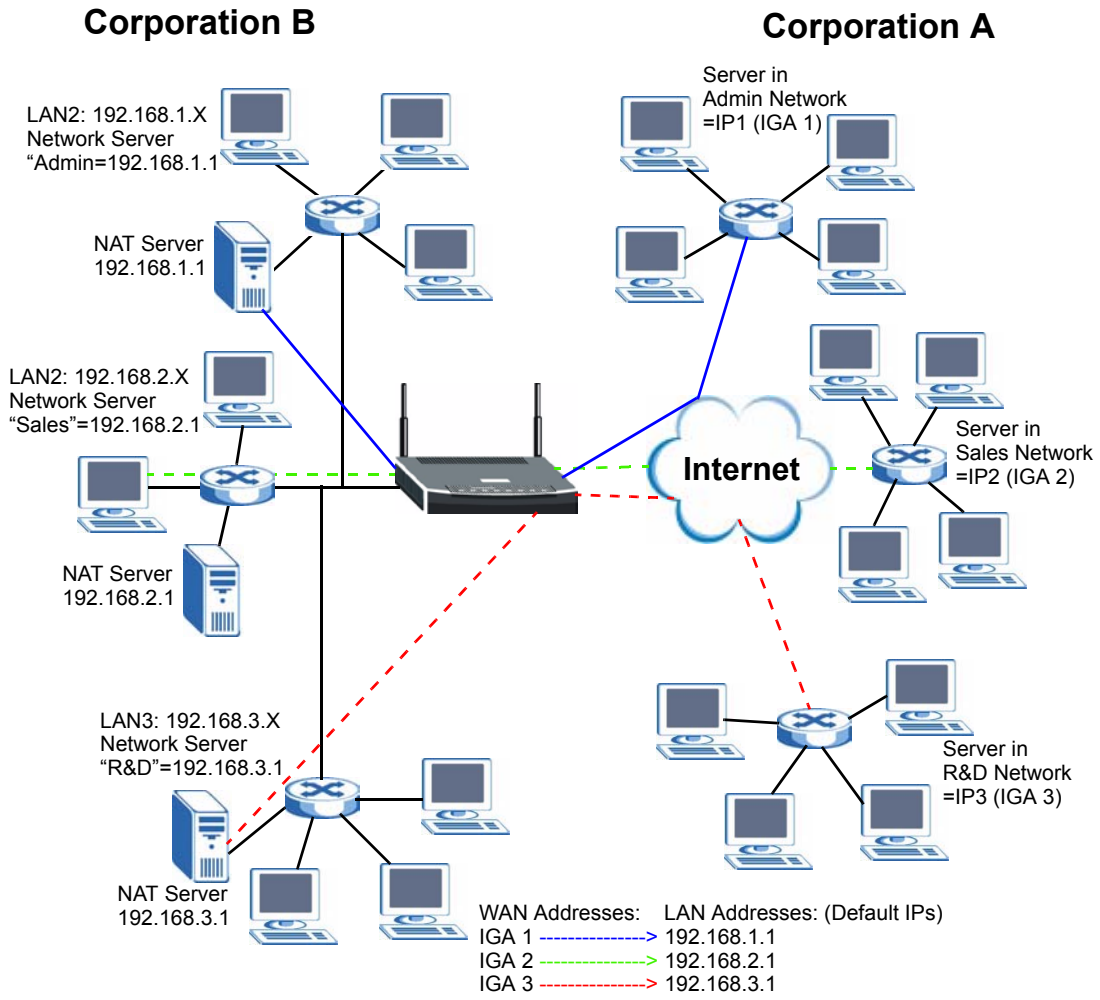
Figure 126 How NAT Works



11.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the ZyXEL Device can communicate with three distinct WAN networks.

Figure 127 NAT Application With IP Alias



11.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL’s Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today’s routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.

- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 46 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1←→ IGA1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

11.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 46 on page 176.

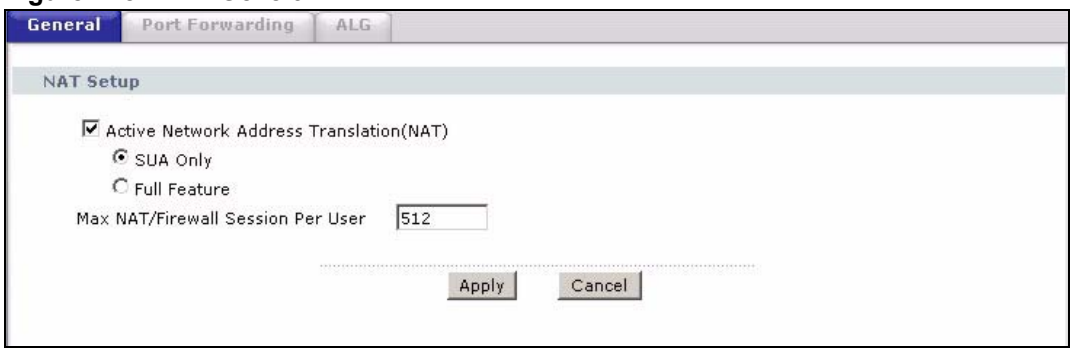
- Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

11.3 NAT General Setup

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

Click **Network > NAT** to open the following screen.

Figure 128 NAT General



The following table describes the labels in this screen.

Table 47 NAT General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the ZyXEL Device. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.4 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

11.4.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

11.4.2 Port Forwarding: Services and Port Numbers

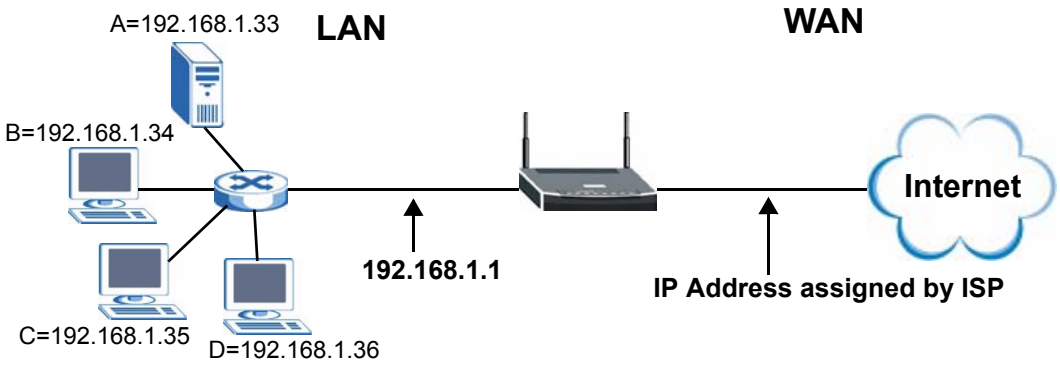
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers and services are shown in Appendix E on page 499. Please refer to RFC 1700 for further information about port numbers.

11.4.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 129 Multiple Servers Behind NAT Example



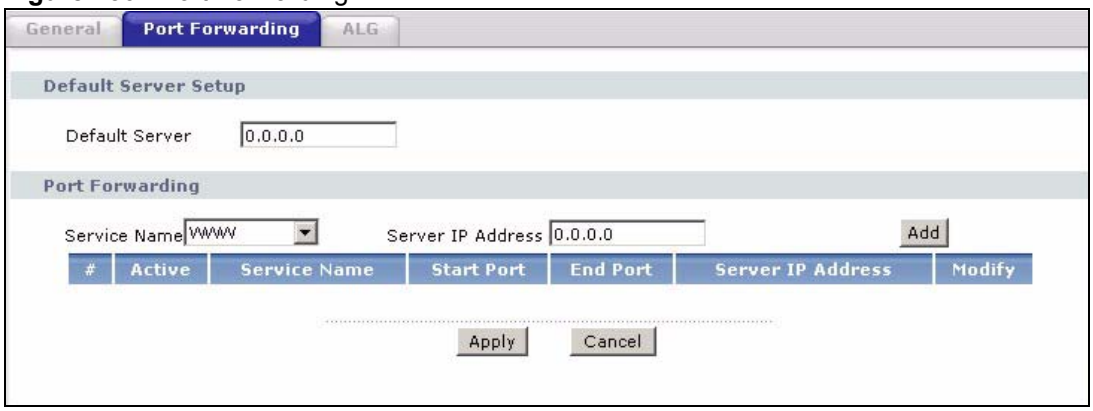
11.5 Configuring Port Forwarding

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **Network > NAT > Port Forwarding** to open the following screen. This screen is available only when you select **SUA only** in the **NAT > General** screen.

See Appendix E on page 499 for port numbers commonly used for particular services.

Figure 130 Port Forwarding



The following table describes the fields in this screen.

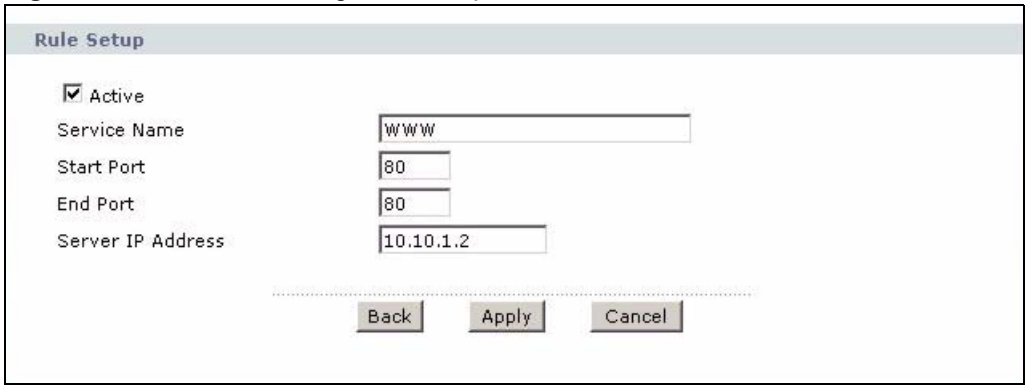
Table 48 Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previous configuration.

11.5.1 Port Forwarding Rule Edit

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 131 Port Forwarding Rule Setup



The following table describes the fields in this screen.

Table 49 Port Forwarding Rule Setup

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

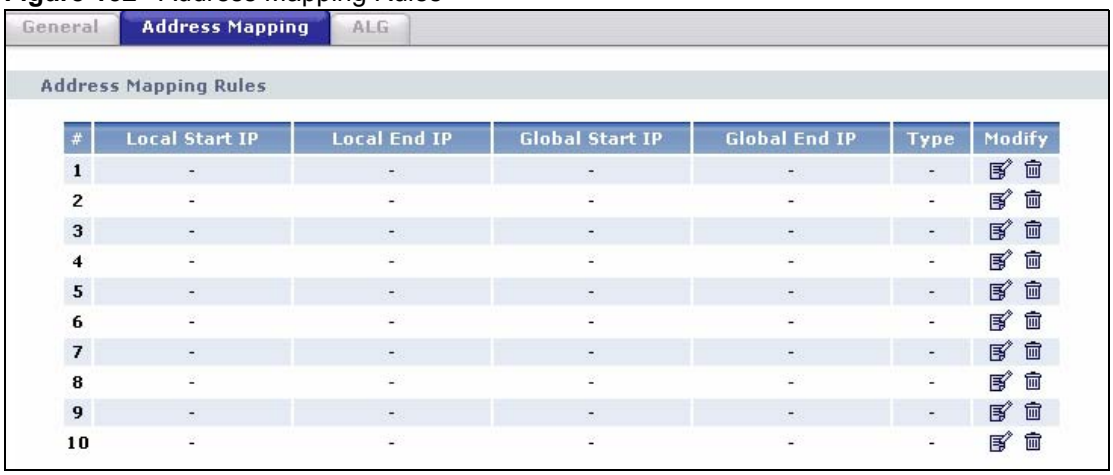
11.6 Address Mapping

The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyXEL Device's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

Figure 132 Address Mapping Rules


General
Address Mapping
ALG
Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -
3 - - - - -
4 - - - - -
5 - - - - -
6 - - - - -
7 - - - - -
8 - - - - -
9 - - - - -
10 - - - - -

The following table describes the fields in this screen.

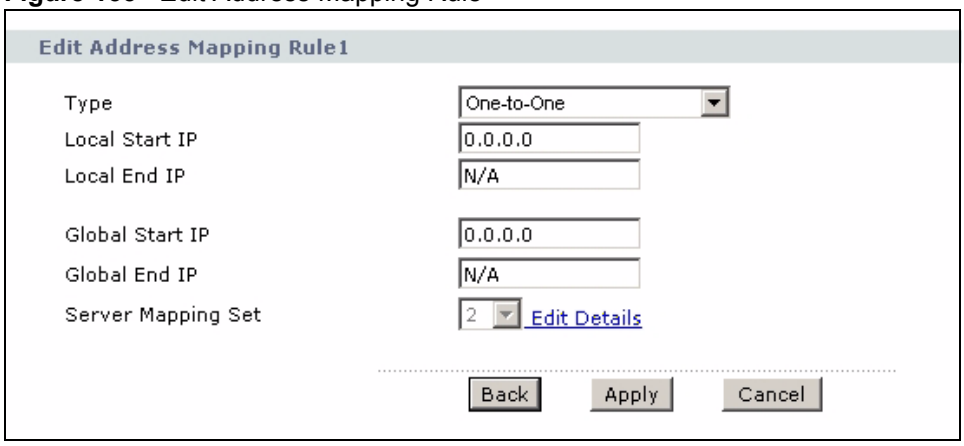
Table 50 Address Mapping Rules

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

11.6.1 Address Mapping Rule Edit

To edit an address mapping rule, click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 133 Edit Address Mapping Rule



The following table describes the fields in this screen.

Table 51 Edit Address Mapping Rule

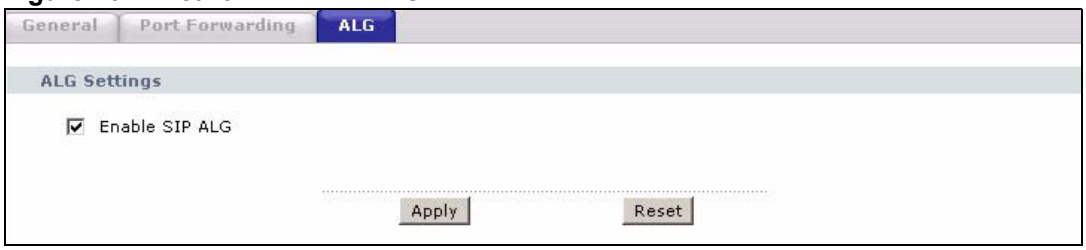
LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a port forwarding set.
Edit Details	Click this link to go to the **Port Forwarding** screen to edit a port forwarding set that you have selected in the **Server Mapping Set** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.6.2 SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device. To access this screen, click **Network > NAT > ALG**.

Figure 134 Network > NAT > ALG



Each field is described in the following table.

Table 52 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to return to previously saved configuration.

12 Voice

This chapter provides background information on VoIP and SIP and explains how to configure your device's voice settings.

12.1 Introduction to VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

12.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

12.2.1 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

12.2.1.1 SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

12.2.1.2 SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

12.2.1.3 SIP Registration

Each ZyXEL Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the ZyXEL Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The ZyXEL Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the ZyXEL Device attempts to register the port immediately.

12.2.1.4 Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

12.2.2 SIP Servers

SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

12.2.2.1 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 135 SIP User Agent

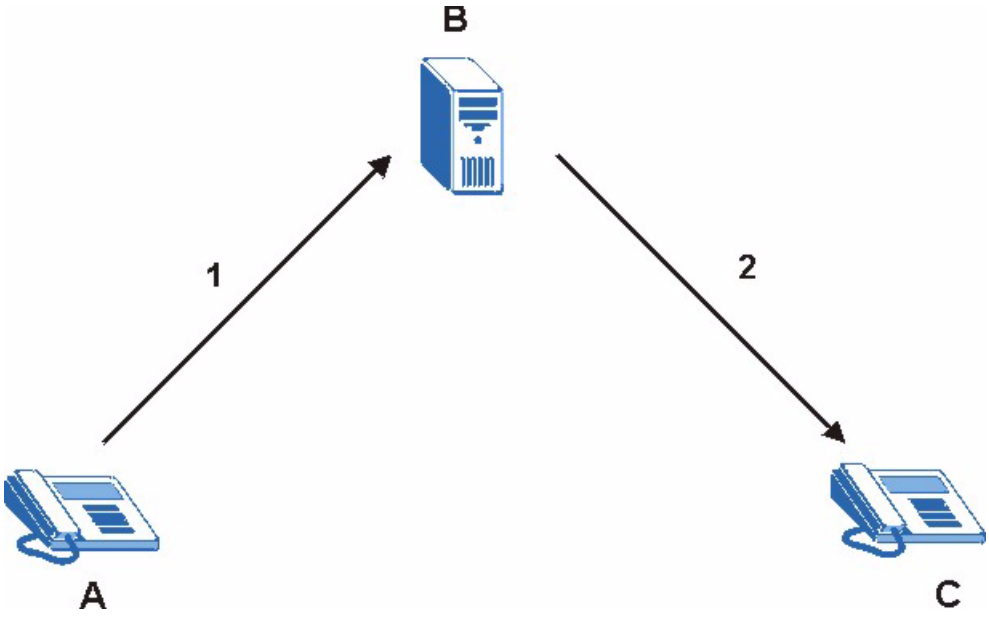
12.2.2.2 SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1. The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).
2. The SIP proxy server forwards the call invitation to **C**.

Figure 136 SIP Proxy Server



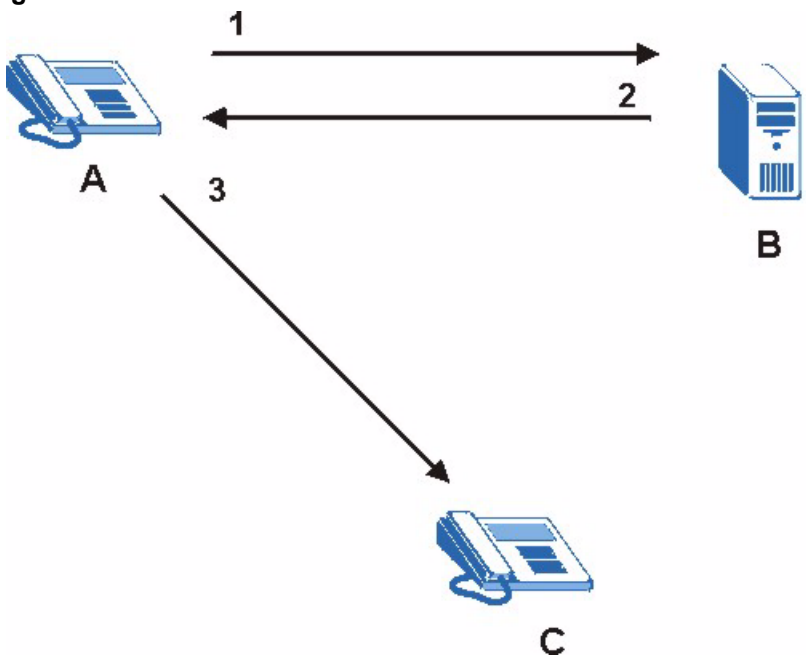
12.2.2.3 SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

1. Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).
2. The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).
3. Client device **A** then sends the call invitation to client device **C**.

Figure 137 SIP Redirect Server



12.2.2.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

12.2.3 RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

12.2.4 Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

12.2.5 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 53 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
	5.Dialogue (voice traffic)	

Table 53 SIP Call Progression (continued)

A		B
6. BYE	→	
	←	7. OK

1. **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.
2. **B** sends a response indicating that the telephone is ringing.
3. **B** sends an OK response after the call is answered.
4. **A** then sends an ACK message to acknowledge that **B** has answered the call.
5. Now **A** and **B** exchange voice media (talk).
6. After talking, **A** hangs up and sends a BYE request.
7. **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

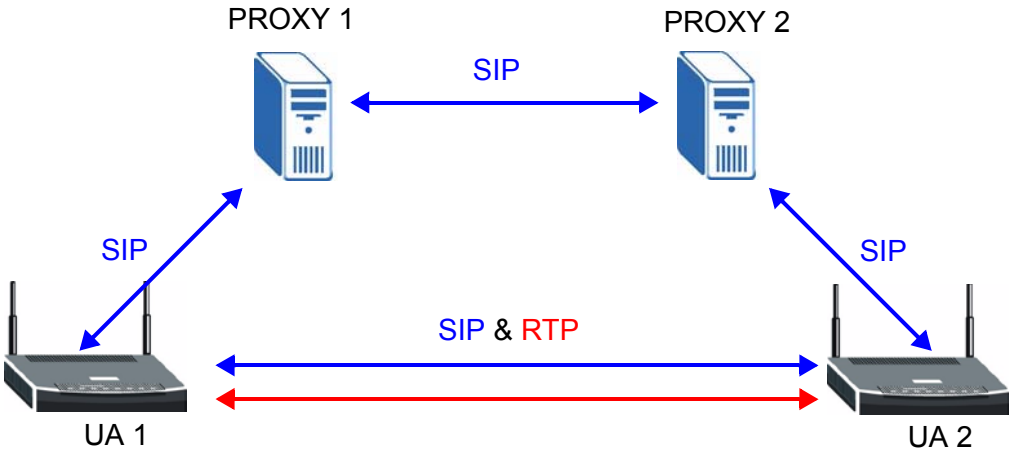
12.2.6 SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phonecall by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

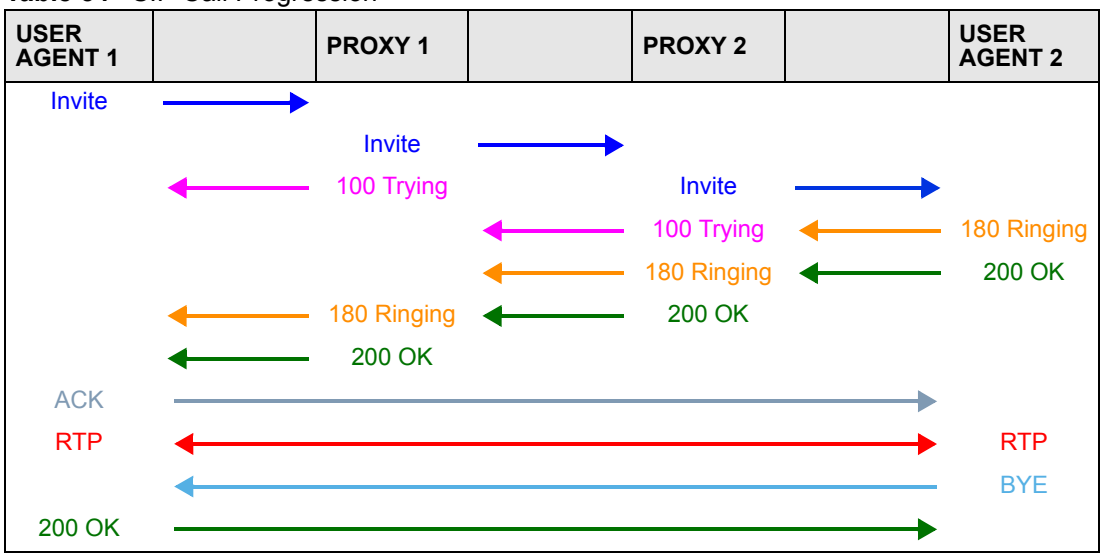
The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 138 SIP Call Through Proxy Servers



The following table shows the SIP call progression.

Table 54 SIP Call Progression



1. **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.
2. **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.
3. **Proxy 2** sends a SIP INVITE request to **User Agent 2**.
4. **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.
5. **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.
6. **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.
7. When **User Agent 2** hangs up, he sends a BYE request.
8. **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

12.2.7 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The ZyXEL Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.

- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

12.2.8 PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[3]

12.2.9 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

12.2.10 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the ZyXEL Device. The ZyXEL Device allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 55 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	128 seconds for all custom tones combined
Time per Individual Tone	20 seconds
Total Number of Tones Recordable	8 You can record up to 8 different custom tones but the total time must be 128 seconds or less.

12.2.10.1 Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1101~1108 on your phone followed by the "#" key.
3. Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.
4. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

3. The ZyXEL Device does not support pulse dialing at the time of writing.

12.2.10.2 Listening to Custom Tones

Do the following to listen to a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1201~1208 followed by the "#" key to listen to the tone.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

12.2.10.3 Deleting Custom Tones

Do the following to delete a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1301~1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

12.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

12.3.1 Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

12.3.2 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[4]

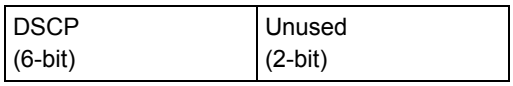
12.3.2.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

4. The ZyXEL Device does not support DiffServ at the time of writing.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 139 DiffServ: Differentiated Service Field



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

12.3.3 VLAN Tagging

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your ZyXEL Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the ZyXEL Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

12.4 SIP Settings Screen

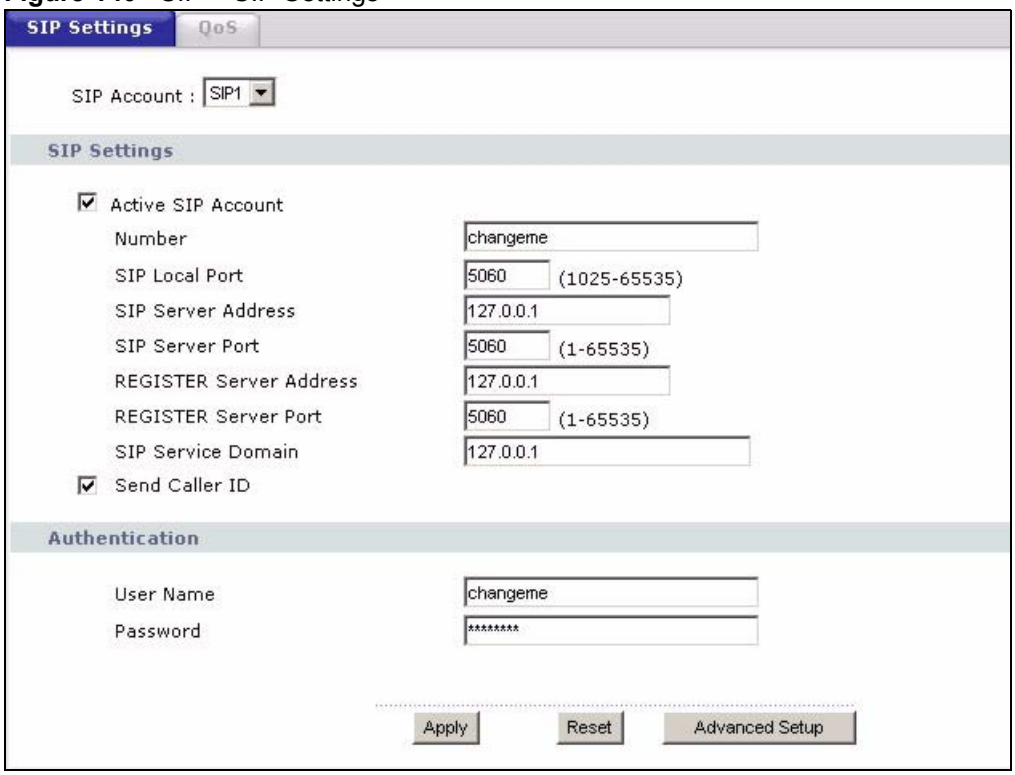
The ZyXEL Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your ZyXEL Device to connect to your VoIP service provider.

If you want to make only peer-to-peer VoIP calls, there is no VoIP service provider involved, so the SIP account information does not have to match a real VoIP service provider's SIP account. You can make up the SIP numbers. However, you should still activate a SIP account and configure its number and map it to a phone port, so that the person you call knows what SIP number you are using and the ZyXEL Device knows to which phone port it should forward an incoming VoIP call. You must use speed dial to make peer-to-peer VoIP calls.

See Section 12.8 on page 200 for how to map a SIP account to a phone port.

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Settings**.

Figure 140 SIP > SIP Settings



Each field is described in the following table.

Table 56 SIP > SIP Settings

LABEL	DESCRIPTION
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
SIP Settings	
Active SIP Account	Select this if you want the ZyXEL Device to use this account. Clear it if you do not want the ZyXEL Device to use this account.
Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
SIP Local Port	Enter the ZyXEL Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.

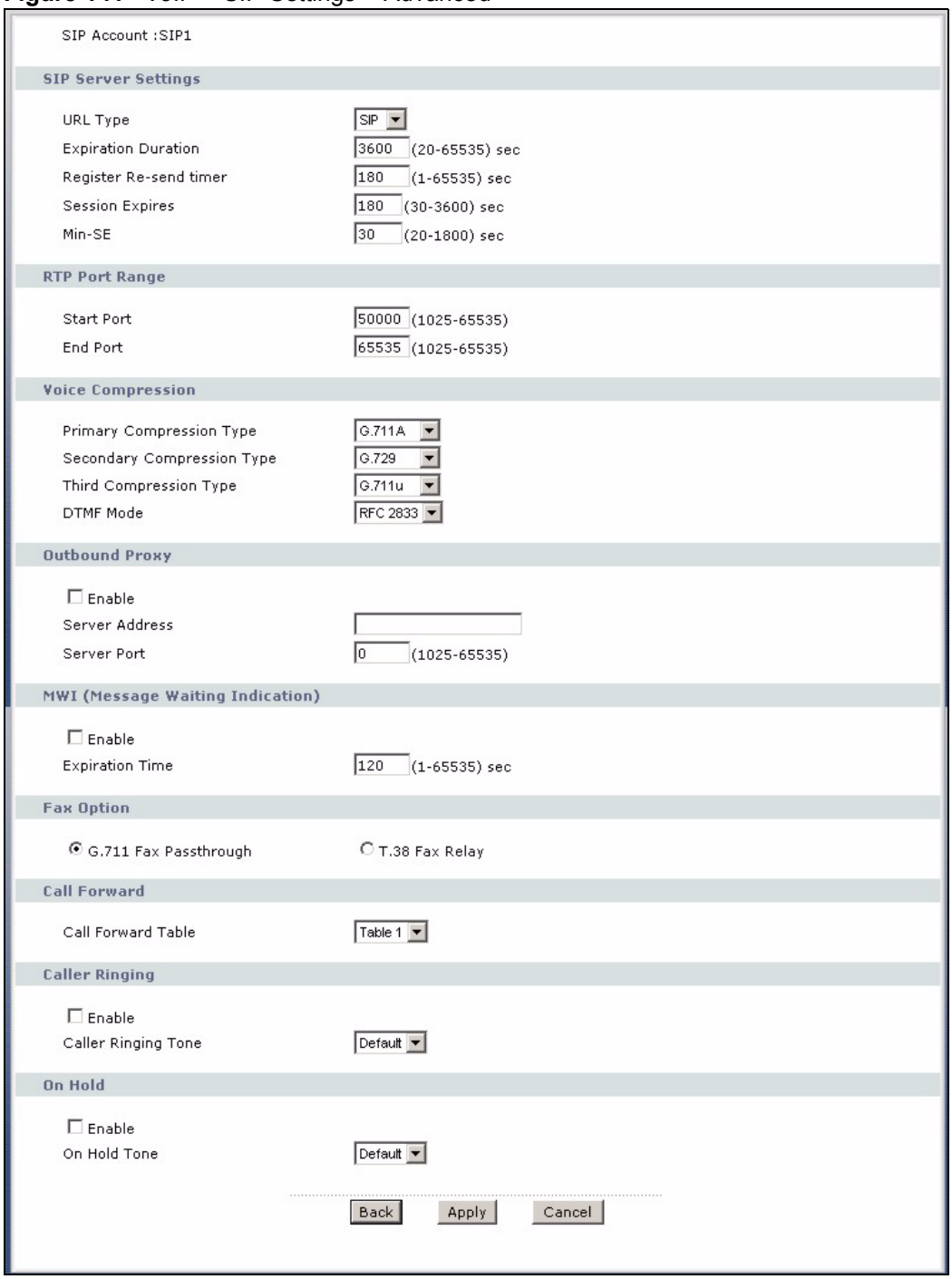
Table 56 SIP > SIP Settings

LABEL	DESCRIPTION
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this SIP account. The **Advanced SIP Setup** screen appears.

12.5 Advanced SIP Setup Screen

Click **VoIP > SIP > SIP Settings** to open the **SIP Settings** screen. Select a SIP account and click **Advanced Setup** to open the **Advanced SIP Setup** screen. Use this screen to maintain advanced settings for each SIP account.

Figure 141 VoIP > SIP Settings > Advanced



Each field is described in the following table.

Table 57 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
SIP Account	This field displays the SIP account you see in this screen.
SIP Server Settings	

Table 57 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the ZyXEL Device accepts.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
Voice Compression	Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.711A** is typically used in Europe. • **G.711u** is typically used in North America and Japan. **G.726** operates at **16**, **24**, **32** or **40** kbps. By contrast, **G.729** only requires 8 kbps. The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.
Primary Compression Type	Select the ZyXEL Device's first choice for voice coder/decoder.
Secondary Compression Type	Select the ZyXEL Device's second choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first choice.
Third Compression Type	Select the ZyXEL Device's third choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first or second choice.
DTMF Mode	Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC 2833** - send the DTMF tones in RTP packets. **PCM** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIP INFO** - send the DTMF tones in SIP messages.
Outbound Proxy	

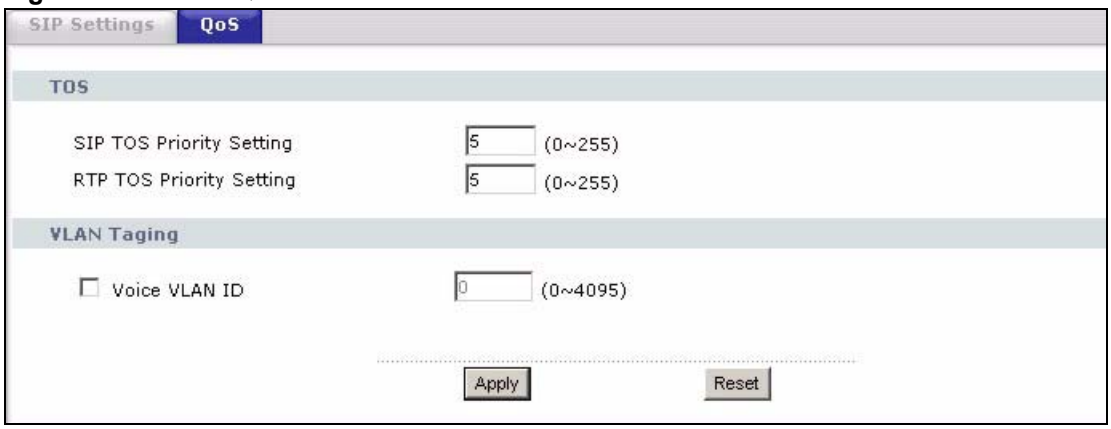
Table 57 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
MWI (Message Waiting Indication)	
Enable	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value for this field, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ZyXEL Device subscribes to the service. Before this time passes, the ZyXEL Device automatically subscribes again.
Fax Option	This field controls how the ZyXEL Device handles fax messages.
G.711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Call Forward	
Call Forward Table	Select which call forwarding table you want the ZyXEL Device to use for incoming calls. You set up these tables in **VoIP** > **Phone Book** > **Incoming Call Policy**.
Caller Ringing	
Enable	Select the check box if you want to specify what tone people hear when they call you. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See Section 12.2.10 on page 191 for more information.
Caller Ringing Tone	Select the tone you want people to hear when they call you. You should set up these tones using IVR first. See Section 12.2.10 on page 191 for more information.
On Hold	
Enable	Select the check box if you want to specify what tone people hear when you put them on hold. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See Section 12.2.10 on page 191 for more information.
On Hold Tone	Select the tone you want people to hear when you put them on hold. You should setup these tones using IVR first. See Section 12.2.10 on page 191 for more information.
Back	Click this to return to the **SIP Settings** screen without saving your changes.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

12.6 SIP QoS Screen

Use this screen to maintain ToS and VLAN settings for the ZyXEL Device. To access this screen, click **VoIP > SIP > QoS**.

Figure 142 SIP > QoS



Each field is described in the following table.

Table 58 SIP > QoS

LABEL	DESCRIPTION
SIP TOS Priority Setting	Enter the priority for SIP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority Setting	Enter the priority for RTP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to RTP traffic that it transmits.
Voice VLAN ID	Select this if the ZyXEL Device has to be a member of a VLAN to communicate with the SIP server. Ask your network administrator, if you are not sure. Enter the VLAN ID provided by your network administrator in the field on the right. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

12.7 Phone

You can configure the volume, echo cancellation and VAD settings for each individual phone port on the ZyXEL Device. You can also select which SIP account to use for making outgoing calls.

12.7.1 Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

12.7.2 Comfort Noise Generation

When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

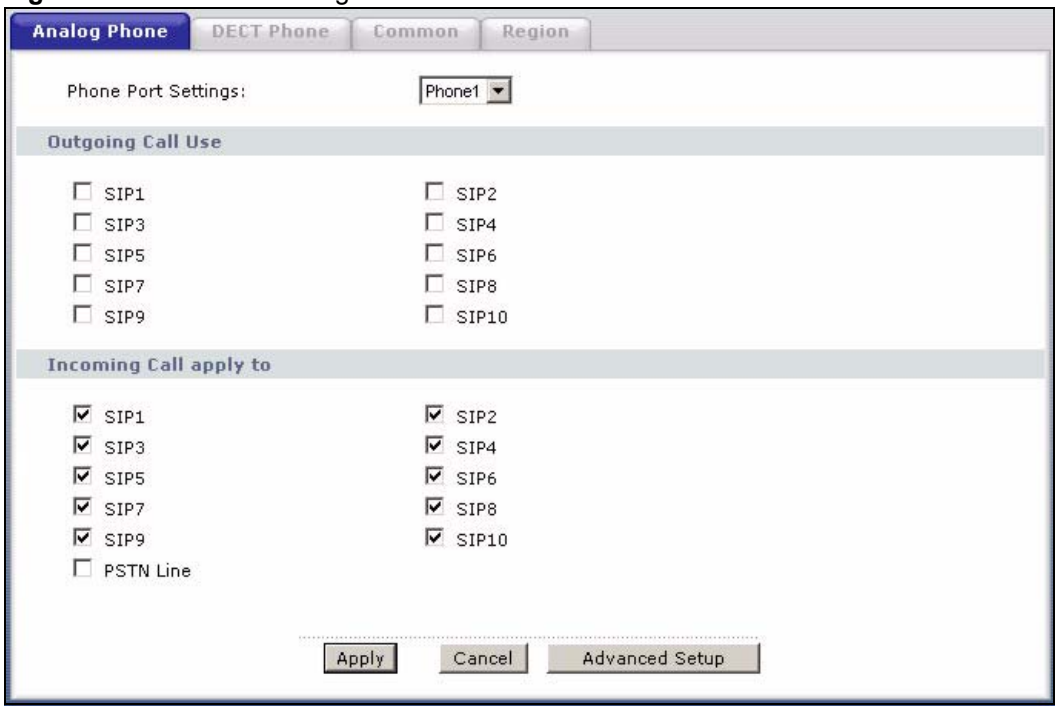
12.7.3 Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

12.8 Analog Phone Screen

Use this screen to control which SIP accounts and PSTN line each phone uses. To access this screen, click **VoIP > Phone > Analog Phone**.

Figure 143 Phone > Analog Phone



Each field is described in the following table.

Table 59 Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Settings	This is the phone port in the ZyXEL Device.
Outgoing Call Use	If you select multiple SIP accounts, the ZyXEL Device tries to use the most recently registered SIP account first. If you do not select a SIP account, you cannot make VoIP calls on the phone connected to this phone port.
SIP1 - SIP10	Select the checkbox of the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.

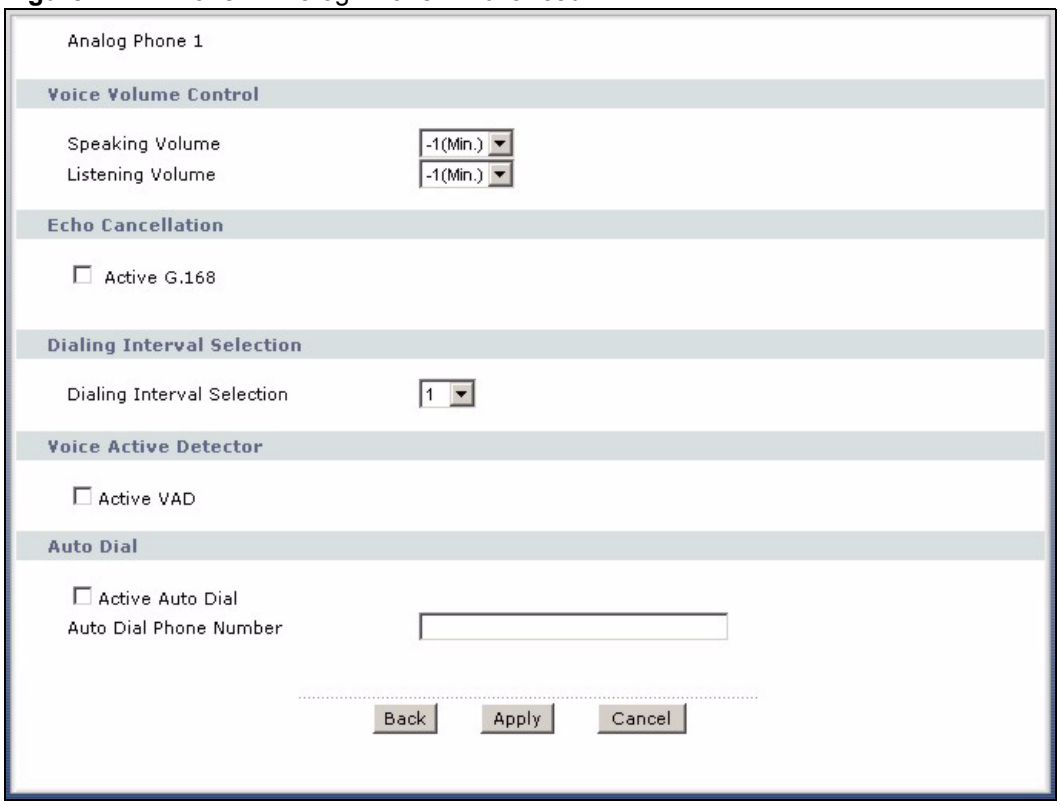
Table 59 Phone > Analog Phone

LABEL	DESCRIPTION
Incoming Call apply to	If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
SIP1 - SIP10	Select the checkbox of the SIP account if you want to receive phone calls for the selected SIP account on this phone port.
PSTN Line	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on this phone port. Note: When the ZyXEL Device does not have power, regardless of the settings you configure, the phone(s) connected to the **PHONE** port can still be used for making PSTN calls. Only one phone can be in use at a time.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this phone port. The **Advanced Analog Phone Setup** screen appears.

12.9 Advanced Analog Phone Setup Screen

Use this screen to edit advanced settings for each phone port. To access this screen, click **Advanced Setup** in **VoIP > Phone > Analog Phone**.

Figure 144 Phone > Analog Phone > Advanced



Each field is described in the following table.

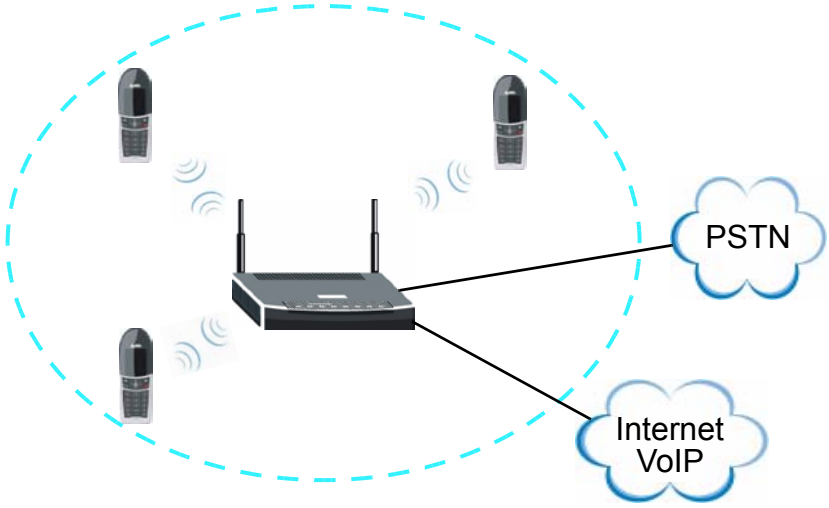
Table 60 Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Analog Phone	This field displays the analog phone port you see in this screen.
Voice Volume Control	
Speaking Volume	Enter the loudness that the ZyXEL Device uses for speech that it sends to the peer device. -1 is the quietest, and 1 is the loudest.
Listening Volume	Enter the loudness that the ZyXEL Device uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest.
Echo Cancellation	
Active G.168	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select **Active Immediate Dial** in **VoIP > Phone > Common**, you can press the pound key (#) to tell the ZyXEL Device to make the phone call immediately, regardless of this setting.
Voice Active Detector	
Active VAD	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
Auto Dial	
Active Auto Dial	Select this if you want the ZyXEL Device to automatically dial the phone number you enter in the **Auto Dial Phone Number** field as soon as you take the phone off the hook.
Auto Dial Phone Number	If you select **Active Auto Dial**, enter the phone number you want the ZyXEL Device to automatically dial in this field.
Back	Click this to return to the **Analog Phone** screen without saving your changes.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

12.10 DECT Base Station Overview

Your ZyXEL Device has a built in Digital Enhanced Cordless Telecommunications (DECT) base station. DECT is an ETSI (European Telecommunications Standards Institute) standard for digital cordless phones which specifies how they transmit, receive and process data and voice communication.

Figure 145 DECT Base Station Overview



The DECT base station follows the Generic Access Profile (GAP). GAP (a subset of DECT) specifies how DECT phones register with a DECT base station. The DECT GAP standard ensures that two different products (a phone and a base station) from different manufacturers can work together. Any phone that supports GAP can make and receive calls through the ZyXEL Device.

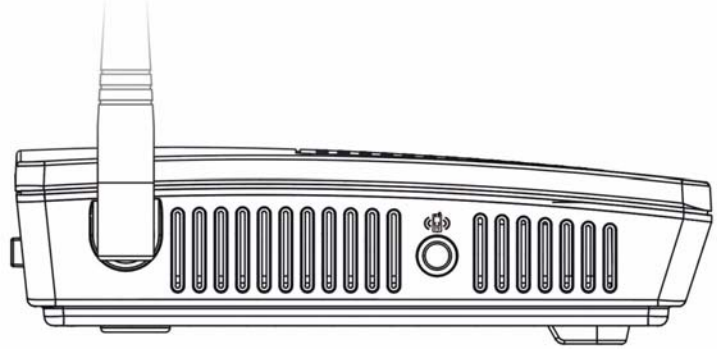
12.10.1 DECT Phone Registration

In order to use your DECT phone with the ZyXEL Device, the DECT phone must register with the ZyXEL Device's DECT base station. Follow these steps to register your DECT phone with the ZyXEL Device.

1. Press down the DECT base station button ( ) on the left side (when facing the LEDs) of your ZyXEL Device for 6 to 11 seconds to put the ZyXEL Device in registration mode.
   Registration mode refers to the state of the ZyXEL Device when it is scanning for DECT phones in its surrounding area. The ZyXEL Device stays in registration mode for 30 seconds.

If you press the DECT base station button for 12 seconds or more, the DECT base station resets and all previously registered DECT phones must be re-registered.

Figure 146 DECT Base Station Button - Side of the ZyXEL Device



2 Put your DECT phone in registration mode. Refer to your DECT phone documentation. When the ZyXEL Device is in registration mode, it scans its surrounding area for DECT phones in registration mode.

Figure 147 DECT Base Station - Phone Registration

Make sure your DECT phone is within range of the ZyXEL Device during the registration process. See Chapter 32 on page 433 for the range of your ZyXEL Device.

3 Enter the Personal Identification Number (PIN) in the DECT phone.
When a ZyXEL Device discovers a DECT phone in registration mode, it sends a request for a PIN. Your DECT phone receives the request and prompts you to enter the PIN. Use your DECT phone's keypad to enter the PIN (you configured on the ZyXEL Device).

The default PIN of the ZyXEL Device is 1234.

4 Repeat steps 1 - 3 to register additional phones. See Chapter 32 on page 433 for the number of DECT phones your ZyXEL Device supports.

12.10.1.1 DECT Base Station Reset

Resetting the DECT base station erases all the details of the DECT phones registered with the ZyXEL Device. You can do this to clear the DECT base station memory of the DECT phones no longer used with the ZyXEL Device, for example if one of your DECT phones is lost.

When you reset the DECT base station, you will need to re-register all the phones that you want to use with the ZyXEL Device.

Resetting the DECT base station does not reset the PIN you use for registering DECT phones. You must use the last PIN you configured to register or re-register your DECT phones.

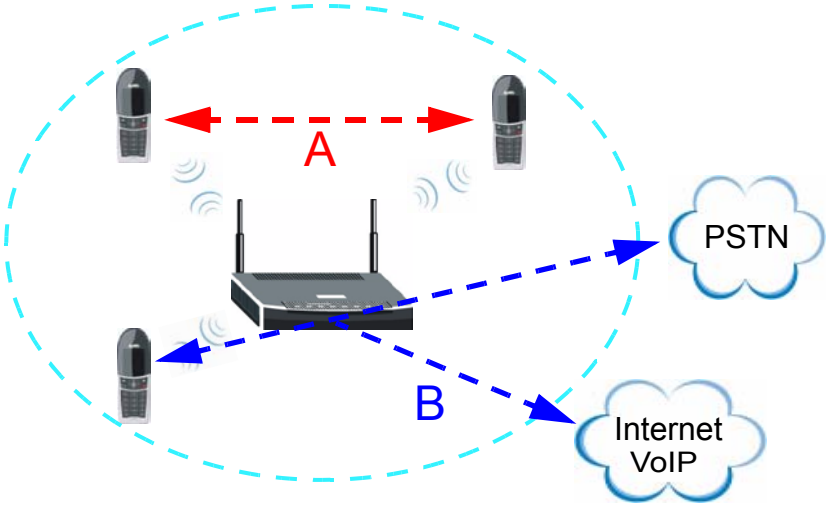
Press the DECT base station button (refer to Figure 146 on page 204) for 12 seconds or more to reset the DECT base station.

12.10.2 Using your DECT Phone

You can use your DECT phone to make calls to other DECT phones registered with the ZyXEL Device (**A**). These calls are referred to as internal calls.

You can also use your DECT phone to make VoIP calls (**B**). For the PSTN models, you can also make calls via the PSTN line (**C**). These types of calls are referred to as external calls.

Figure 148 Using Your DECT Phone



The following table summarizes the types and number of calls you can make with your DECT phones via the ZyXEL Device.

Table 61 DECT Phone Calls Summary

TYPE OF CALL	DESCRIPTION	LIMITS
Internal	A call between two DECT phones registered with the ZyXEL Device DECT base station.	Two calls.
External	A call from the DECT phone to or from a VoIP or a PSTN caller.	Two calls.
3 Way Conference	A call between two DECT phones registered with the ZyXEL Device base station and an external connection.	One call.
The ZyXEL Device allows up to four DECT phones to be active at one time.		

The ZyXEL Device does not control how your DECT phone distinguishes between internal and external calls. Typically, a DECT phone has a button labeled **int** to indicate an internal call. Consult your DECT phone documentation for differences in making internal and external calls.

12.10.2.1 DECT Phones - Internal Calls

To make internal calls, you need to know the phone numbers of the other DECT phones registered with the ZyXEL Device. The ZyXEL Device assigns numbers based on the order that the DECT phones registered with the ZyXEL Device's DECT base station. The first DECT phone that registered with the ZyXEL Device's DECT base station receives the number **1**, the second the number **2**, and so on up to the last registered DECT phone.

Refer to your DECT phone documentation for specific details regarding your phone's calling functions.

12.10.2.2 DECT Phones - External Calls

To make external calls, follow the same procedure as with the analog phone connected to the ZyXEL Device. You must also:

- Specify the SIP accounts for incoming and outgoing VoIP calls.
- Specify whether each DECT phone should receive calls on the PSTN line.

12.10.2.3 DECT Phones - Supplementary Services

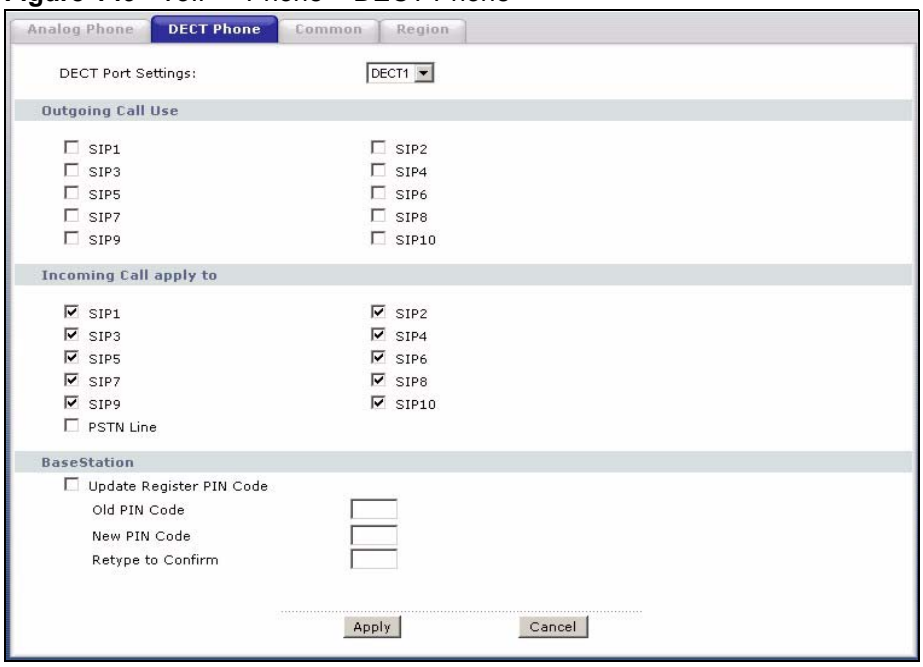
There are two ways to perform supplementary phone services like call waiting, conference calling and so on.

- Via the handset - refer to your DECT phone documentation.
- Via the flash key function - refer to Section 12.12.1 on page 209. On most DECT phone models the flash key is the "R" key.

12.10.3 DECT Phone Screen

Use this screen to configure your DECT base station settings. To access this screen, click **VoIP > Phone > DECT Phone**.

Figure 149 VoIP > Phone > DECT Phone



Each field is described in the following table.

Table 62 VoIP > Phone > DECT Phone

LABEL	DESCRIPTION
DECT Port Settings	Select the DECT phone you want to see in this screen. If you change this field, the screen automatically refreshes.
Outgoing Call Use	If you select multiple SIP accounts, the ZyXEL Device tries to use the most recently registered SIP account first.
SIP1 - SIP10	Select the checkbox of the SIP account you want to use when making outgoing calls with your DECT phone.
Incoming Call apply to	If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
SIP1 - SIP10	Select the checkbox of the SIP account if you want to receive phone calls for the selected SIP account on your DECT phone.
PSTN Line	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on your DECT phones.
Base Station	
Update Register PIN Code	Select this to update the PIN code of the DECT phone. The default PIN code is **1234**. If you are changing the PIN code for the first time, enter **1234** in the **Old PIN Code** field. Note: When the PIN code changes, phones already registered with the ZyXEL Device will have to re-register when they are turned off and turned on again.
Old PIN Code	Enter the existing PIN code. The PIN code can be from 1 to 4 digits long and is limited to numbers 0 to 9.
New PIN Code	Enter the new PIN code. The PIN code is 1 to 4 digits long and is limited to numbers 0 to 9.
Retype to Confirm	Retype the new PIN code.

Table 62 VoIP > Phone > DECT Phone

LABEL	DESCRIPTION
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

12.11 Common Phone Settings Screen

Use this screen to activate and deactivate immediate dialing and set up call fallback. To access this screen, click **VoIP > Phone > Common**.

Figure 150 Phone > Common

Each field is described in the following table.

Table 63 Phone > Common

LABEL	DESCRIPTION
Immediate Dial	
Active Immediate Dial	Select this if you want to use the pound key (#) to tell the ZyXEL Device to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialing Interval Selection** in **VoIP > Phone > Analog Phone > Advanced Setup**. If you select this, dial the phone number, and then press the pound key. The ZyXEL Device makes the call immediately, instead of waiting. You can still wait, if you want.
Call Fallback	
Force to PSTN if SIP unregistered	Select this to have the ZyXEL Device redirect outgoing calls to the PSTN connection if there are no SIP accounts registered on the ZyXEL Device. When you try to make a SIP call, but no SIP account is registered, the ZyXEL Device uses the phone line connected to the PSTN port to make the call.
Force to SIP if PSTN unplugged	Select this to have the ZyXEL Device redirect outgoing calls to the registered SIP account if the ZyXEL Device is not connected to the PSTN network. When you try to make a PSTN call, but the PSTN port on the ZyXEL Device is unplugged, the ZyXEL Device uses the phone port's registered SIP account to make the call.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

12.12 Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The ZyXEL Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding (see Section 12.15 on page 214)
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb

To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

12.12.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the ZyXEL Device.

You can invoke all the supplementary services by using the flash key.

12.12.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 64 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.

Table 64 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

12.12.2.1 European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

12.12.2.2 European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.
  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.
  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.
  Press the flash key and then “2”.

12.12.2.3 European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
3. After you hear the ring signal or the second party answers it, hang up the phone.

12.12.2.4 European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call.
3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4 Hang up the phone to drop the connection.
5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

12.12.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 65 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

12.12.3.1 USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

12.12.3.2 USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

12.12.3.3 USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1 Press the flash key to put the caller on hold.
2 When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
3 After you hear the ring signal or the second party answers it, hang up the phone.

12.12.3.4 USA Three-Way Conference

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call (to party B).
3 When party B answers the second call, press the flash key to create a three-way conversation.
4 Hang up the phone to drop the connection.
5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.
6 If you want to go back to the three-way conversation, press the flash key again.
7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

12.13 Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the ZyXEL Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 151 VoIP > Phone > Region

Each field is described in the following table.

Table 66 VoIP > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the ZyXEL Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. **Europe Type** - use supplementary phone services in European mode **USA Type** - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

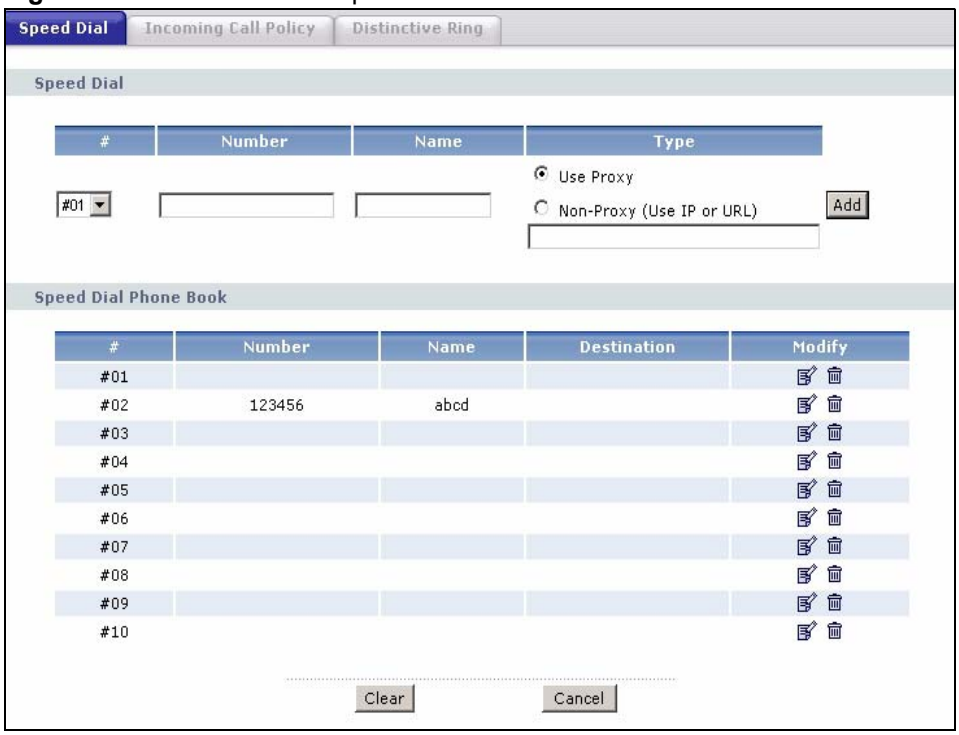
12.14 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. You also have to create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. To access this screen, click **VoIP > Phone Book > Speed Dial**.

In peer-to-peer calls, you call another VoIP device directly without going through a VoIP service provider's SIP server. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The ZyXEL Device sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

Figure 152 Phone Book > Speed Dial



Each field is described in the following table.

Table 67 Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Name	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.

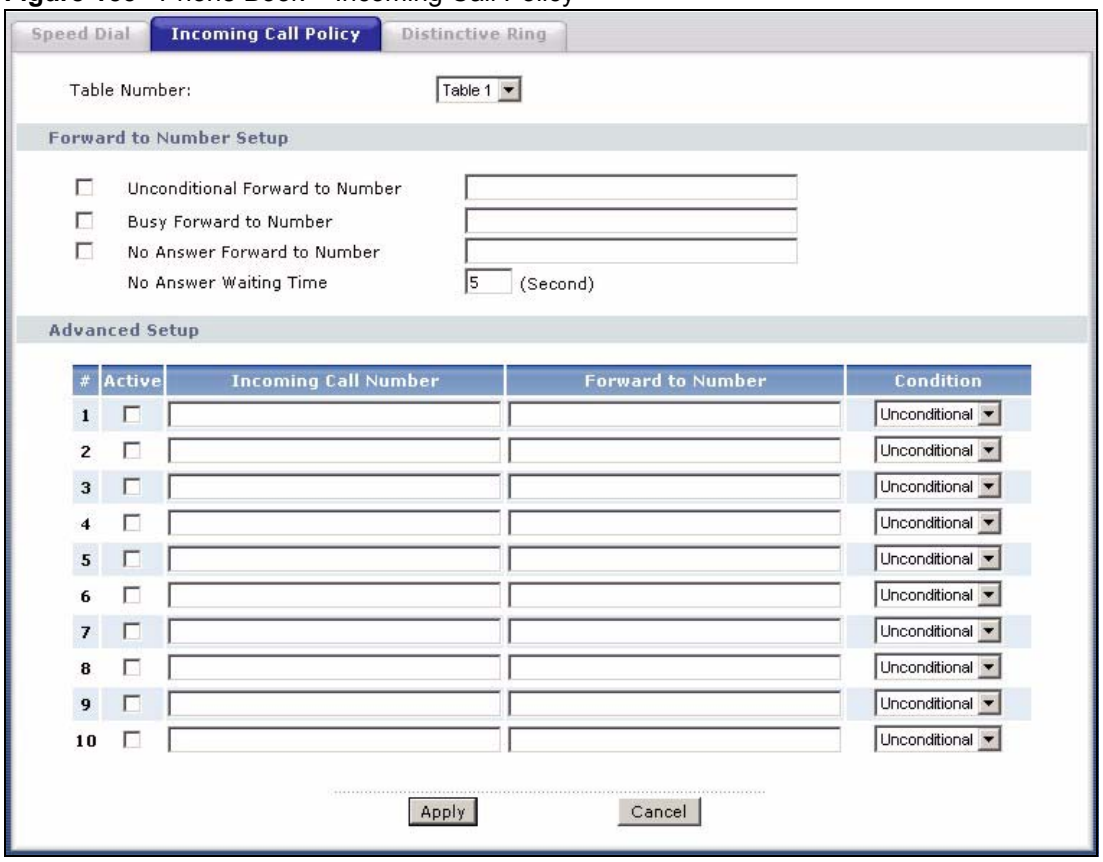
Table 67 Phone Book > Speed Dial

LABEL	DESCRIPTION
Type	Select **Use Proxy** if you want to use one of your SIP accounts to call this phone number. Select **Non-Proxy (Use IP or URL)** if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below.
Add	Click this to use the information in the **Speed Dial** section to update the **Speed Dial Phone Book** section.
Speed Dial Phone Book	Use this section to look at all the speed-dial entries and to erase them.
Speed Dial	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.
Name	This field displays the name of the party you call when you dial the speed-dial number.
Destination	This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the **Type** field in the **Speed Dial** section.)
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** icon to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click the **Remove** icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

12.15 Incoming Call Policy Screen

Use this screen to maintain rules for handling incoming calls. You can block, redirect, or accept them. To access this screen, click **VoIP > Phone Book > Incoming Call Policy**.

Figure 153 Phone Book > Incoming Call Policy



You can create two sets of call-forwarding rules. Each one is stored in a call-forwarding table. Each field is described in the following table.

Table 68 Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
Table Number	Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes.
Forward to Number Setup	The ZyXEL Device checks these rules, in the order in which they appear, after it checks the rules in the **Advanced Setup** section.
Unconditional Forward to Number	Select this if you want the ZyXEL Device to forward all incoming calls to the specified phone number, regardless of other rules in the **Forward to Number** section. Specify the phone number in the field on the right.
Busy Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Waiting Time**.) Specify the phone number in the field on the right.
No Answer Waiting Time	This field is used by the **No Answer Forward to Number** feature and **No Answer** conditions below. Enter the number of seconds the ZyXEL Device should wait for you to answer an incoming call before it considers the call is unanswered.
Advanced Setup	The ZyXEL Device checks these rules before it checks the rules in the **Forward to Number** section.

Table 68 Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it only follows the first one that applies.
Activate	Select this to enable this rule. Clear this to disable this rule.
Incoming Call Number	Enter the phone number to which this rule applies.
Forward to Number	Enter the phone number to which you want to forward incoming calls from the **Incoming Call Number**. You may leave this field blank, depending on the **Condition**.
Condition	Select the situations in which you want to forward incoming calls from the **Incoming Call Number**, or select an alternative action. **Unconditional** - The ZyXEL Device immediately forwards any calls from the **Incoming Call Number** to the **Forward to Number**. **Busy** - The ZyXEL Device forwards any calls from the **Incoming Call Number** to the **Forward to Number** when your SIP account already has a call connected. **No Answer** - The ZyXEL Device forwards any calls from the **Incoming Call Number** to the **Forward to Number** when the call is unanswered. (See **No Answer Waiting Time**.) **Block** - The ZyXEL Device rejects calls from the **Incoming Call Number**. **Accept** - The ZyXEL Device allows calls from the **Incoming Call Number**. You might create a rule with this condition if you do not want incoming calls from someone to be forwarded by rules in the **Forward to Number** section.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

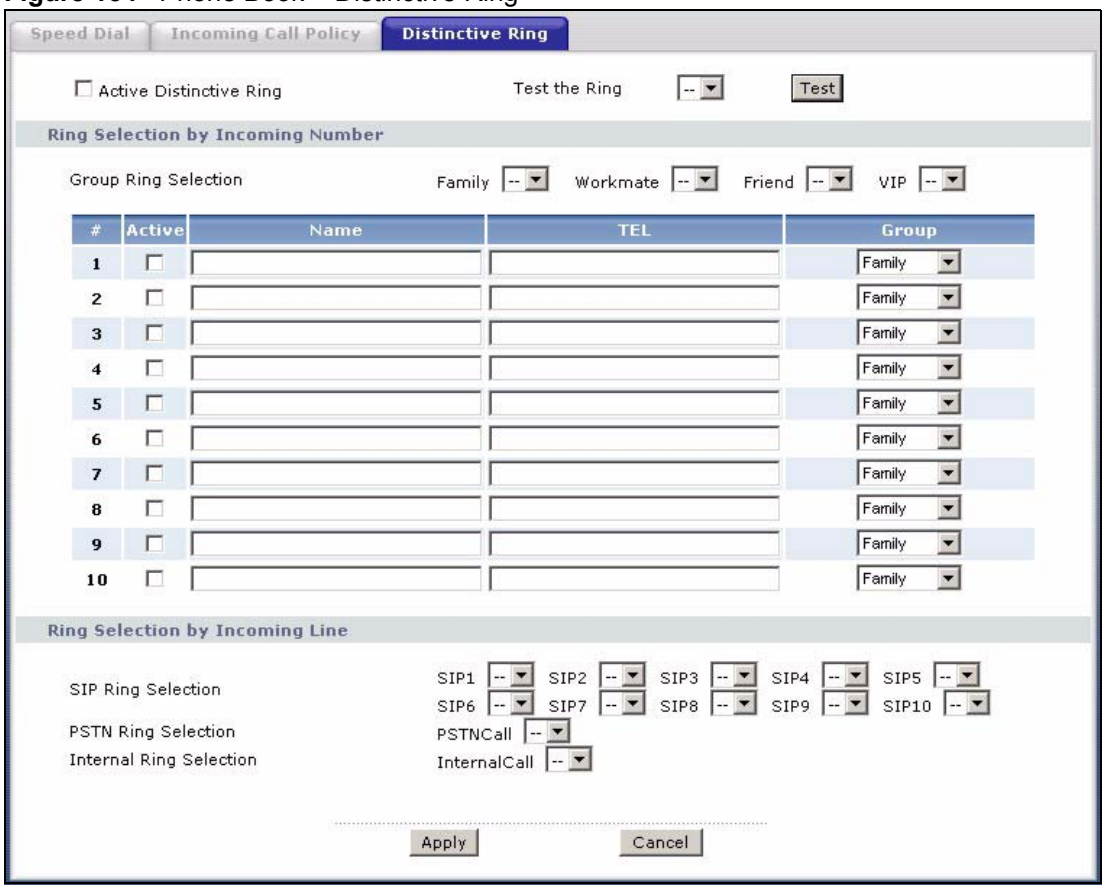
12.16 Distinctive Ring Screen

This screen lets you specify ring types for calls from particular numbers. The ring types vary by ring duration and stop ring duration (the time gap between the rings). Any standard phone is compatible with this feature.

When an incoming call comes in, the ZyXEL Device checks whether it is from any of the phone numbers you set up in this screen. If the number matches an enabled entry, the ZyXEL Device sends the corresponding ring to your phone. You can also configure different rings for calls coming into various SIP accounts, coming into the PSTN line and internal calls.

To access this screen, click **VoIP > Phone Book > Distinctive Ring**.

Figure 154 Phone Book > Distinctive Ring



Each field is described in the following table.

Table 69 Phone Book > Distinctive Ring

LABEL	DESCRIPTION
Active Distinctive Ring	Select this if you want to activate the distinctive ring feature. You also have to enable individual entries.
Test the Ring	Use the drop down list box to select the ring tone you would like to hear.
Test	Click this to listen to the ring. All the phones connected to the ZyXEL Device ring when you click this button.
Ring Selection by Incoming Number	Use this section to first assign rings to groups and then assign phone numbers to those groups.
Family	Select the ring for callers in your family group.
Workmate	Select the ring for callers in your workmate group.
Friend	Select the ring for callers in your friend group.
VIP	Select the ring for callers in your VIP group.
#	This is a read only index number for the phone numbers you assign to different groups.
Active	Select this to enable your selected distinctive ring for this phone number.
Name	Type a name for the associated telephone number.
TEL	Type the telephone number you want to add to a group.
Group	Select a group for the telephone number you entered. You can select **Family**, **Workmate**, **Friend** or **VIP**.

Table 69 Phone Book > Distinctive Ring

LABEL	DESCRIPTION
Ring Selection By Incoming Line	You can also select distinctive rings based on whether a call comes from the registered SIP accounts, the PSTN line, or another phone connected to the ZyXEL Device (internal). Note: The ZyXEL Device will check whether the incoming phone number is part of any of the groups assigned above before checking the incoming line.
SIP Ring Selection	Select a ring for each registered SIP account.
PSTN Ring Selection	Select a ring for PSTN calls.
Internal Ring Selection	Select a ring for internal calls.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12.17 PSTN Line

With PSTN line you can make and receive regular PSTN phone calls. Use a prefix number to make a regular call. When the device does not have power, you can make regular calls without dialing a prefix number.

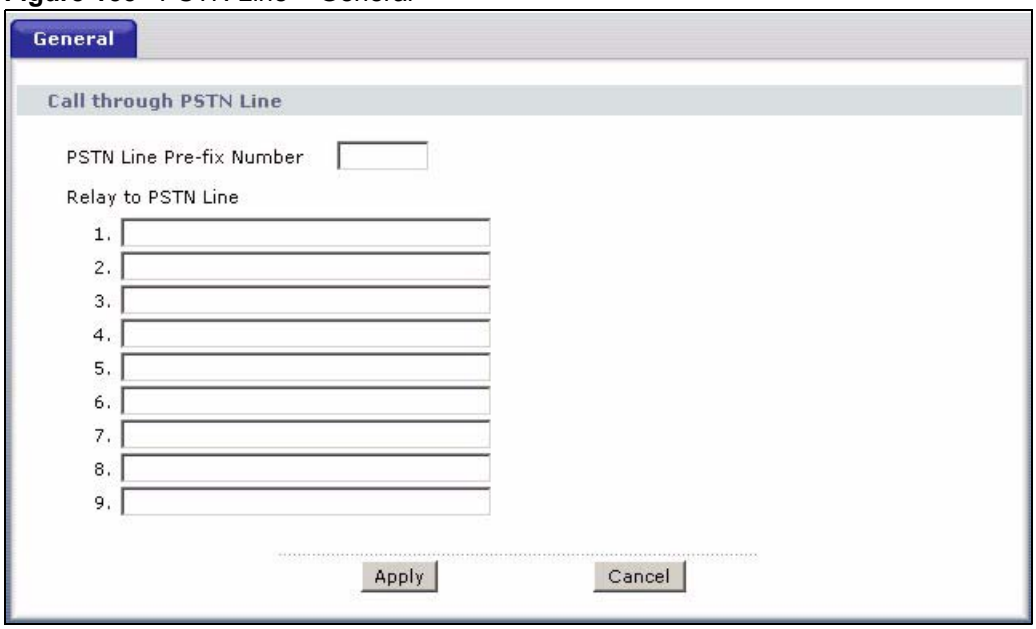
When the ZyXEL Device does not have power, the phone(s) connected to the **PHONE** port can still be used for making PSTN calls. Only one phone can be in use at a time.

You can also use the **PSTN Line** screen to specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

12.18 PSTN Line Screen

Use this screen to set up the PSTN line you use to make regular phone calls. To access this screen, click **VoIP > PSTN Line > General**.

Figure 155 PSTN Line > General



Each field is described in the following table.

Table 70 PSTN Line > General

LABEL	DESCRIPTION
PSTN Line Pre-fix Number	Enter a prefix (up to seven numbers) you dial before you dial the phone number, if you want to make a regular phone call while one of your SIP accounts is registered. These numbers tell the ZyXEL Device that you want to make a regular phone call.
Relay to PSTN Line	Enter phone numbers (for regular calls, not VoIP calls) that you want to dial without the prefix number. For example, you should enter emergency numbers. The number (1 - 9) is not a speed-dial number. It is just a sequential value that is not associated with any phone number.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

13

VoIP Trunking

Use these screens to configure VoIP trunking on your ZyXEL Device.

13.1 VoIP Trunking Overview

VoIP trunking connects an IP network (like the Internet) and the Public Switched Telephone Network (PSTN). PSTN includes the world's circuit-switched telephone network which is composed of fixed and mobile telephones. VoIP trunking allows you to create VoIP links which PSTN (Public Switched Telephone Network) callers can use to:

- Make phone calls via the Internet - Make a PSTN call to the ZyXEL Device and it forwards the call to any SIP based VoIP phone.
- Save on long distance calls - The ZyXEL Device creates a VoIP link which can be used to connect to a PSTN phone in another country, province, region and so on.

Similarly, VoIP callers can:

- Make calls to PSTN subscribers at reduced cost - Connect to the ZyXEL Device via VoIP and the ZyXEL Device forwards the call to a PSTN phone.

Creating a link over the IP network requires two VoIP devices. VoIP trunking scenarios vary depending on how the VoIP devices work together and how they receive or forward PSTN calls. The following sections describe the details of VoIP trunking.

13.2 VoIP Trunking and Security

Your ZyXEL Device provides two types of authentication to prevent unauthorized callers from using it for VoIP trunking.

13.2.1 Auto Attendant and Authentication

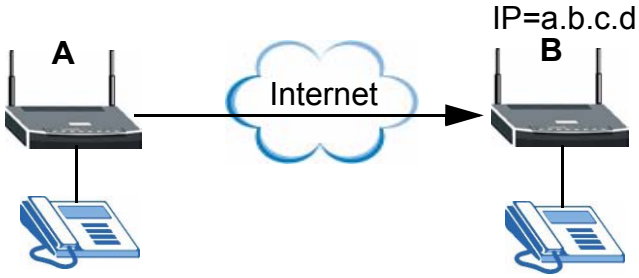
Auto attendant is the ZyXEL Device's name for a service which controls settings specific to VoIP trunking. Most importantly it controls authentication for VoIP trunking. Auto attendant authentication is similar to using a calling card with a PIN (Personal Identification Number). Your ZyXEL Device can be configured so that it prompts callers to enter a PIN (via the phone pad) in order to process any call forwarding requests.

Other settings controlled by the auto attendant include a time limit to decide whether you want to forward a call from the ZyXEL Device or call the phone directly connected to the ZyXEL Device. When you call into your ZyXEL Device you can request to forward a call to another phone number simply by dialing that number. If you don't dial any number within a specified time limit (for example 5 seconds) then the phone directly connected to the ZyXEL Device rings. It also controls the time limit you have between dialing digits of a phone number.

13.2.2 Peer Call Authentication

VoIP devices can make peer calls to each other by using the IP address instead of a SIP number to establish a call. The advantage of this is that you do not need to pay a VoIP service provider. VoIP devices that connect using an IP address are referred to here as peer devices. A local peer device is where the VoIP call originates and a remote peer device is where the VoIP call ends. In the following figure, local peer device (**A**) connects to a remote peer device (**B**) via the IP address of **B**.

Figure 156 Peer Devices Connecting



A peer-to-peer call doesn't require any authentication, however, authentication is required when you request the remote peer device to forward a call. The remote peer device has a list of accounts, each consisting of a username and password, which are allowed to use the remote peer device to forward calls. These accounts make up an incoming authentication list.

The local peer device has a corresponding list of outgoing authentication accounts. These accounts consist of the IP address of a remote peer device, the port number to communicate over as well as a username and password to use for authentication. An outgoing authentication account must match an incoming authentication account's username and password in order for the remote device to forward calls. The following table shows example entries for incoming and outgoing authentication. The bolded entries must match in order for authentication between two peer devices to occur.

Table 71 Matching Incoming and Outgoing Authentication

ACCOUNT DETAILS	LOCAL PEER DEVICE	REMOTE PEER DEVICE
Outgoing Authentication		
Username	localDeviceA	localDeviceB
Password	passwordA	passwordB
Incoming Authentication		
Username	userone	localDeviceA
Password	userpassword	passwordA

13.3 Call Rules

Call rules automate the forwarding of calls, first to a remote peer device and then to PSTN phones. This is used when you make frequent calls to several PSTN numbers in the same geographic area that start with the same numbers (for example an area code). If there is a remote peer device in that area, you can set up a VoIP link to it and have it forward the calls to PSTN phones. This works by configuring a pattern that the ZyXEL Device can recognize. A pattern is just the initial string of digits shared by the phone numbers. The following table shows the relationship between the phone numbers you want to call, the pattern you want to configure and the rule you want to set up.

Table 72 Call Rules

FREQUENTLY CALLED PSTN NUMBERS	PATTERN	CALL RULE
1-555-555-4321 1-555-544-5678 1-555-432-8888	1555	Set up a peer call to a remote peer device to forward calls starting with the numbers 1555.
1-111-555-4321 1-111-544-5678 1-111-432-8888	1111	Set up a peer call to a remote peer device to forward calls starting with the numbers 1111.

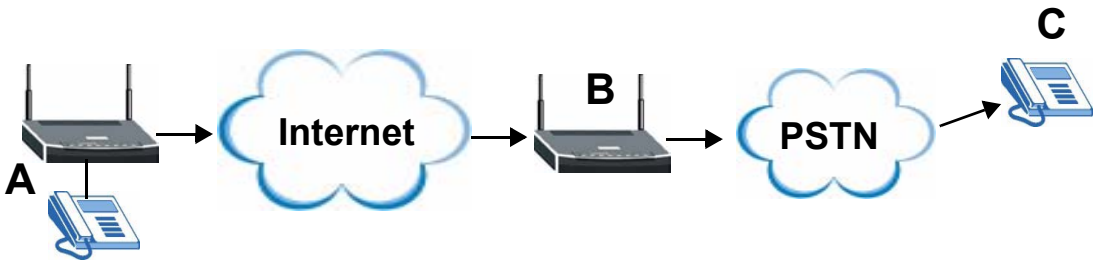
13.4 VoIP Trunking Scenarios

There are several different VoIP trunking scenarios.

13.4.1 VoIP Phone To PSTN Phone

A VoIP phone **A** makes a call to the ZyXEL Device **B** via VoIP. **B** forwards the call to a PSTN phone **C**. **A** can be an analog phone connected to the ZyXEL Device or any other phone capable of making calls over the IP network.

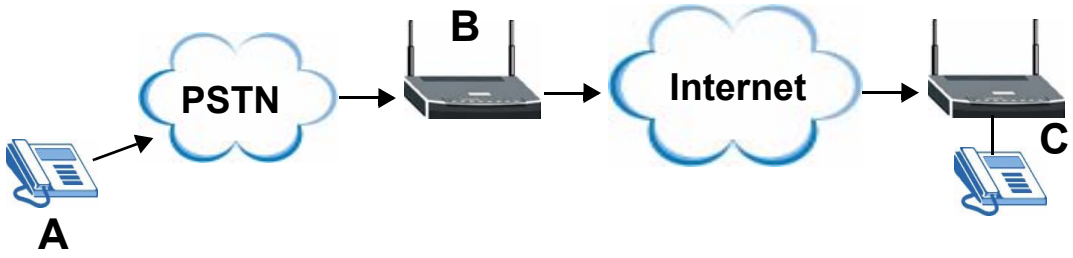
Figure 157 VoIP Phone To PSTN Phone



13.4.2 PSTN Phone To VoIP Phone

A PSTN phone **A** makes a call to the ZyXEL Device **B**. **B** connects **A** to a VoIP phone **C** over the IP network.

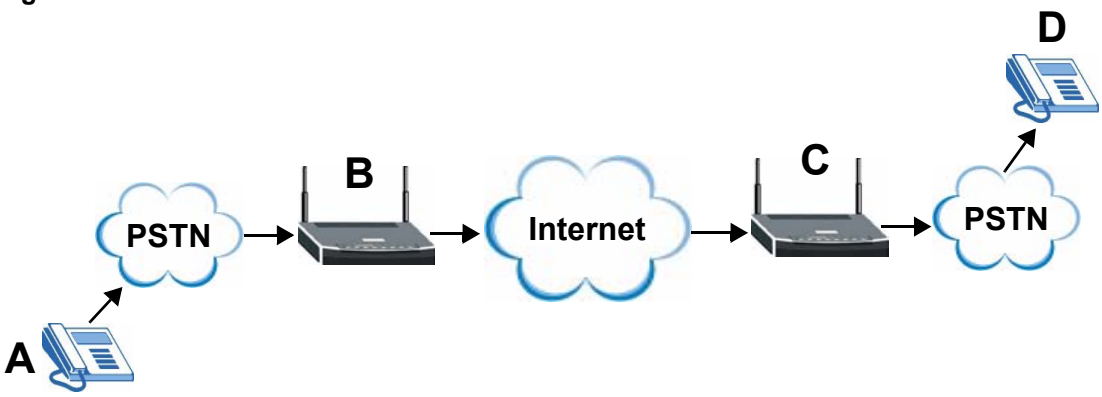
Figure 158 PSTN Phone To VoIP Phone



13.4.3 PSTN Phone To PSTN Phone via VoIP

A PSTN phone **A** makes a call to the ZyXEL Device **B**. **B** connects to a peer device **C** and **C** forwards the call to a PSTN phone **D**.

Figure 159 PSTN Phone To PSTN Phone via VoIP

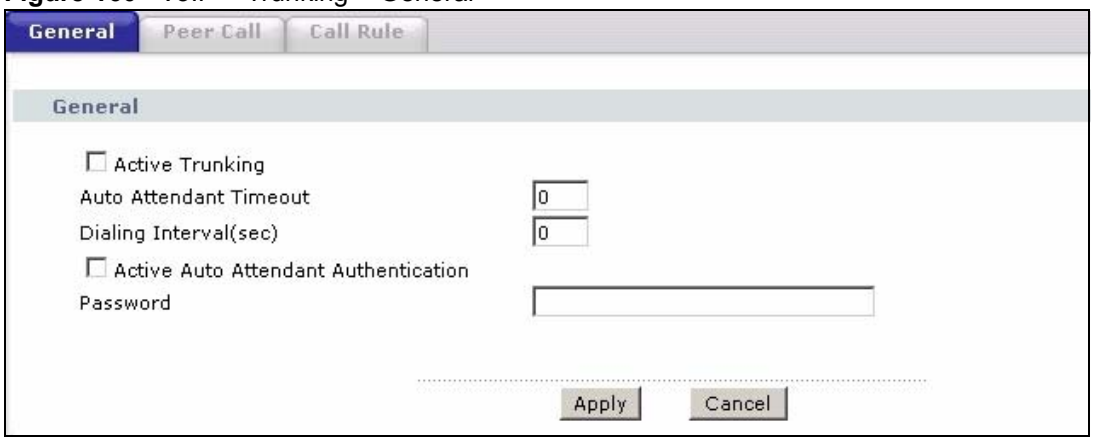


13.5 Trunking General Screen

Use this screen to enable VoIP trunking. Click **VoIP** > **Trunking** > **General**.

VoIP Trunking requires the following additional configuration in the **VoIP > SIP > SIP Settings > Advanced Setup** screen: **Voice Compression** field needs to be set to **G.729** and **DTMF Mode** field needs to be set to **SIP INFO**.

Figure 160 VoIP > Trunking > General



Each field is described in the following table.

Table 73 VoIP > Trunking > General

LABEL	DESCRIPTION
Enable Trunking	Select this to turn on VoIP trunking on your ZyXEL Device.
Auto Attendant Timeout	This setting determines how long the ZyXEL Device waits for a caller to enter a phone number (to which the ZyXEL Device forwards the call) when it receives the call. Enter a value from 1 to 255 seconds. If you do not dial any number(s) before the auto attendant times out, the phone directly connected to the ZyXEL Device rings. If you enable **Auto Attendant Authentication**, after you dial a phone number, the ZyXEL Device prompts you to enter the password.
Dialing Interval(sec)	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. The default value is 3 seconds and entering 0 does not change the default. Enter a value from 1 to 255 seconds.
Enable Auto Attendant Authentication	Select this to enable authentication for calls coming into your ZyXEL Device. This is similar to enabling a PIN (Personal Identification Number) that callers must enter to forward calls via your ZyXEL Device.
Password	This is the PIN callers have to enter via their phone pad when dialing into your ZyXEL Device to forward calls through it. Enter a number between 1 and 32 digits long.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to reset the fields.

13.6 Trunking Peer Call Screen

Use this screen to set up outgoing authentication accounts for forwarding calls through peer devices (without proxy) and incoming authentication accounts for forwarding calls from peer devices. To access this screen, click **VoIP > Trunking > Peer Call**.

Figure 161 VoIP > Trunking > Peer Call

Each field is described in the following table.

Table 74 VoIP > Trunking > Peer Call

LABEL	DESCRIPTION
Outgoing Authentication	You need to set up accounts for the peer devices you use in VoIP trunking. This is the IP address of the remote peer device, as well as the username and password needed to authenticate with the remote peer device.
#	This is an index number of your outgoing authentication accounts.
Name	Enter a descriptive name for the remote peer device of this account. For example, if the peer device is located in London, you might enter **London** as the account name. This name is used when you configure call rules in the **VoIP > Trunking > Call Rules** screen.
Username	Enter the username needed to authenticate at the remote peer device. The remote peer device must have the same username in an incoming authentication entry in order to authenticate your connection. Enter up to 32 alphanumeric characters.

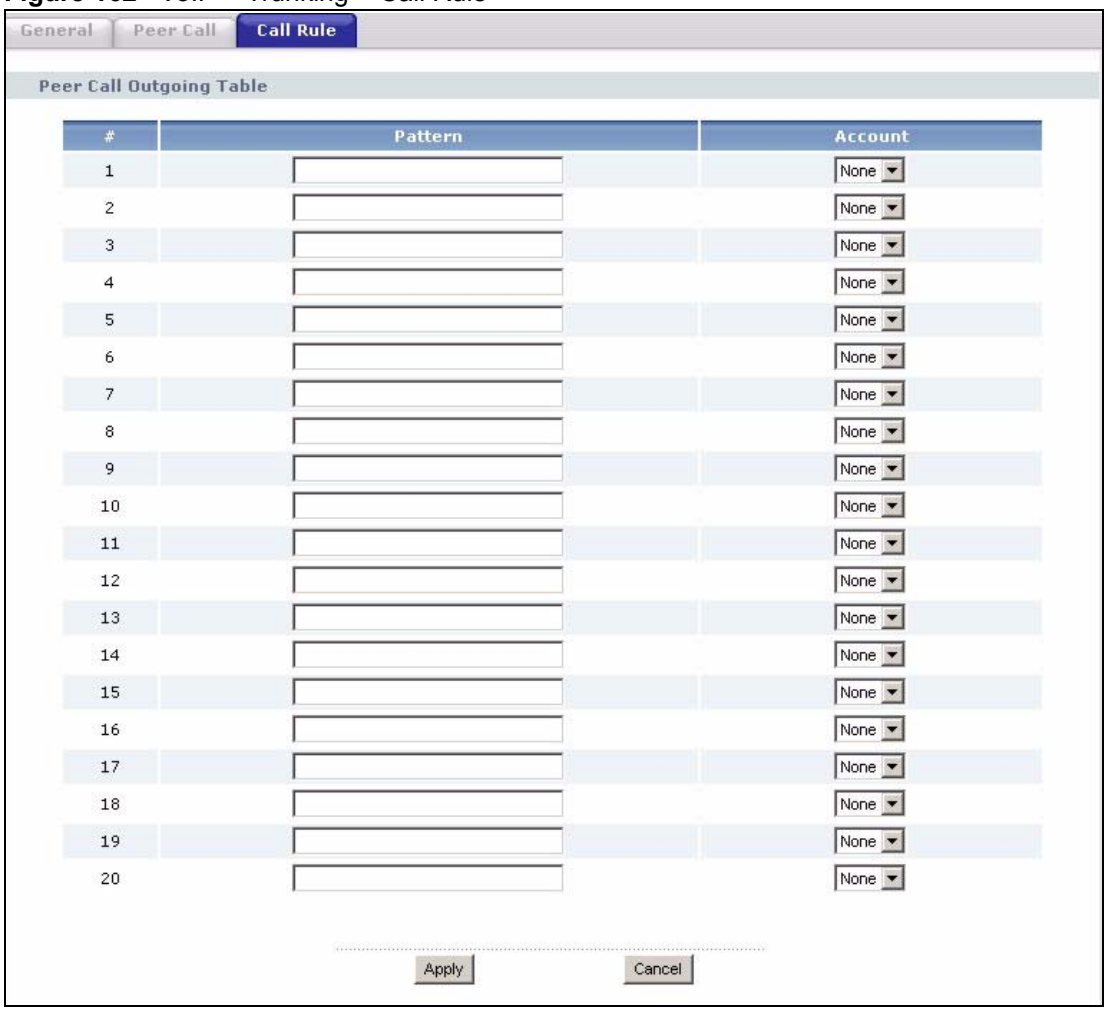
Table 74 VoIP > Trunking > Peer Call (continued)

LABEL	DESCRIPTION
Password	Enter the corresponding password for the username you entered. The remote peer device must have the same password in an incoming authentication entry in order to authenticate your connection. Enter up to 32 alphanumeric characters.
Peer IP	Enter the IP address of the remote peer device which you want to connect to.
Peer Port	Enter the port number through which your ZyXEL Device will connect to the remote peer device. The default value is the standard port for VoIP communication. Do not change this value unless the remote peer device does not follow the standard.
Incoming Authentication	You can set up multiple accounts which are allowed to use your ZyXEL Device for VoIP trunking. When peer devices want to forward calls through your ZyXEL Device, this is the list your ZyXEL Device checks to see if the user has the right to complete the call.
#	This is the index number of the incoming authentication accounts.
Username	Enter a username for the account. This username is used to authenticate peer devices forwarding calls through the ZyXEL Device. Enter up to 32 alphanumeric characters.
Password	Enter the password for the corresponding username. This password is used to authenticate peer devices calling the ZyXEL Device. Enter up to 32 alphanumeric characters.
Apply	Click this to apply your settings to the ZyXEL Device.
Cancel	Click this to reset the fields to their last saved values.

13.7 Trunking Call Rule Screen

Use this screen to set up rules that determine which peer VoIP device your call will be forwarded to. To access this screen, click **VoIP > Trunking > Call Rule**.

Figure 162 VoIP > Trunking > Call Rule



Each field is described in the following table.

Table 75 VoIP > Trunking > Call Rule

LABEL	DESCRIPTION
#	This is a read-only index number of the call rules.
Pattern	A **Pattern** is used when you call your ZyXEL Device from a PSTN phone and want to use it to create a VoIP link to a remote peer device which will forward the call to a PSTN phone. A **Pattern** is a string of digits your ZyXEL Device uses to determine whether or not to send the call to a peer VoIP device. For example, if you want to use trunking to call phone numbers which start with the number “555”, then enter 555 in this field. Enter up to 32 numeric characters. If the number you dial does not match any of the patterns you configured, then you can still use your ZyXEL Device to forward calls to VoIP phones. Simply dial the SIP number of the VoIP phone you want to call.
Account	Select the outgoing authentication account you set up in the **Peer Call** screen. This account is used to direct your call to the correct remote peer device and to authenticate you. Select **None** to disable this forwarding rule.
Apply	Click this to apply your settings to the ZyXEL Device.
Cancel	Click this to reset the fields.

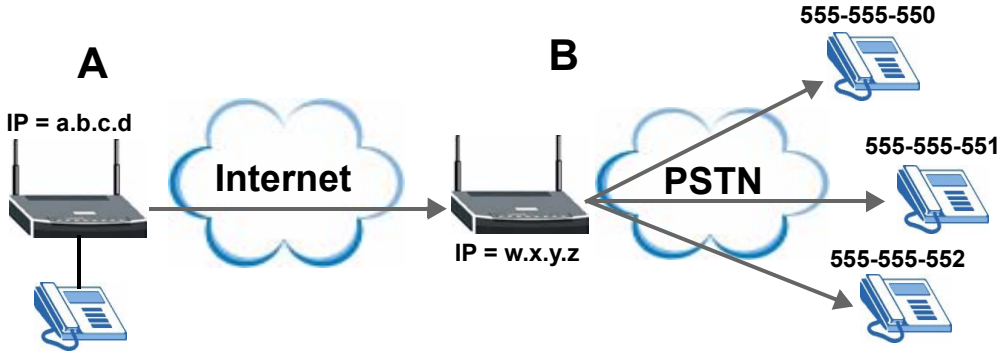
13.8 VoIP Trunking Example: VoIP to PSTN

This example shows how to configure VoIP to PSTN trunking to save on long distance calls.

13.8.1 Background Information

A company has its headquarters in city **A** and a branch office in city **B**. The headquarters often needs to call salespeople employed at the branch office. The sales employees often work away from the office and have PSTN phones (mobile or land based). The two offices have VoIP trunking devices and want to use VoIP trunking to save on calls from the headquarters to their sales team. The head office has a public IP address **a.b.c.d** and the branch office has a public IP address **w.x.y.z**.

Figure 163 VoIP to PSTN Example



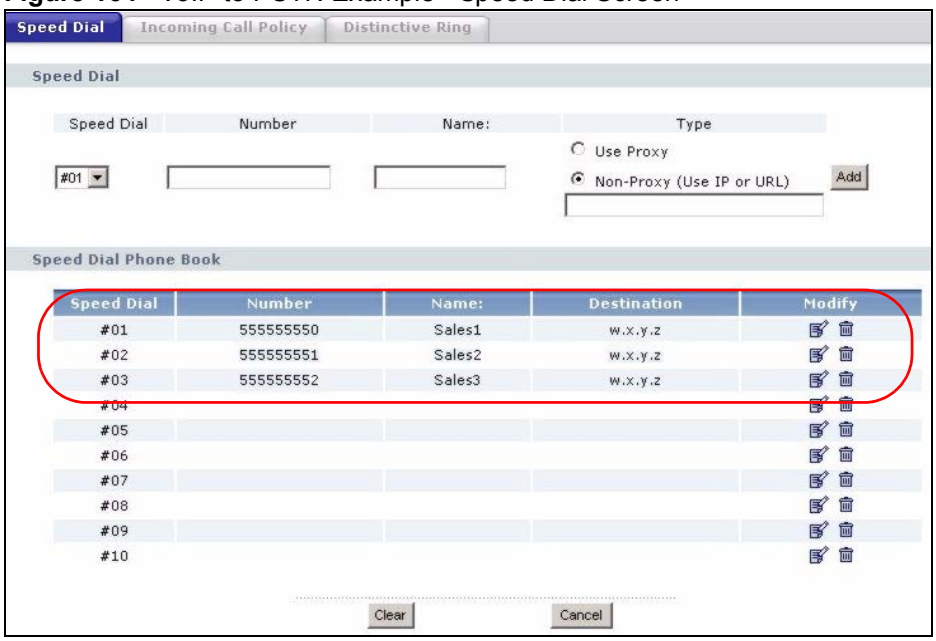
The proposed solution is to establish a peer-to-peer call between the two ZyXEL Devices and have the branch office ZyXEL Device forward calls to the sales team members via PSTN.

13.8.2 Configuration Details: Outgoing

The ZyXEL Device (at headquarters) from which the call originates needs to have the following configuration settings:

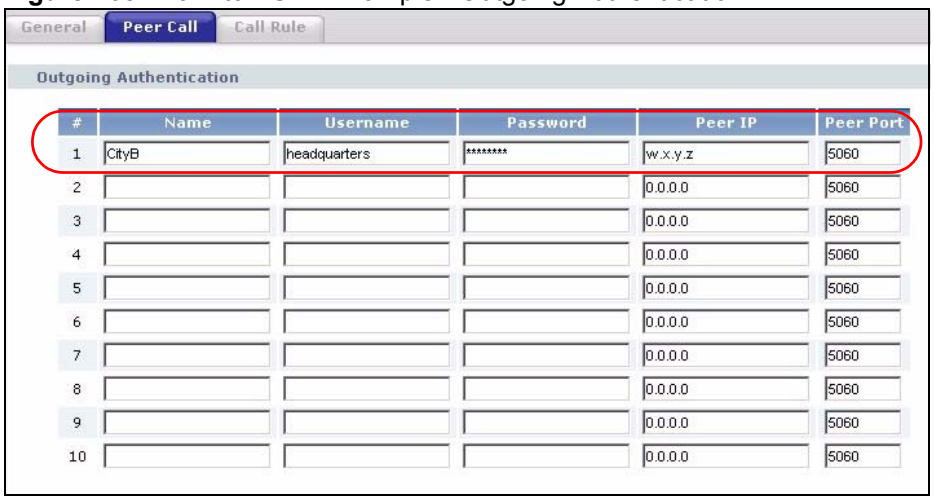
1. Speed dial entries need to be set up for the numbers headquarters wants to call. The destination field of these entries is the IP address of the branch office ZyXEL Device. This must be a non-proxy IP address. The numbers are the phone numbers of the sales team members. This can be configured in the **VoIP** > **Phone Book** > **Speed Dial** screen.

Figure 164 VoIP to PSTN Example - Speed Dial Screen



2 An outgoing authentication account needs to be configured. This account consists of the IP address and port number of the branch office ZyXEL Device as well as the username and password for authentication. This username and password must match the incoming authentication account username and password on the branch office ZyXEL Device. The name of this rule is "CityB" referring to the branch office ZyXEL Device. In this example the username is "headquarters" and the password is "password". This can be configured in the **VoIP** > **Trunking** > **Peer Call** screen.

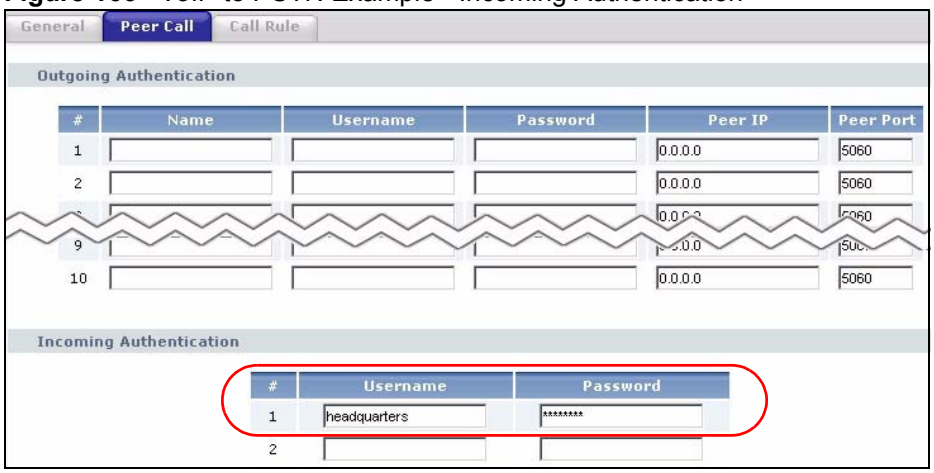
Figure 165 VoIP to PSTN Example - Outgoing Authentication



13.8.3 Configuration Details: Incoming

The branch office ZyXEL Device needs to have an incoming authentication account configured. This consists of a username and password. This account must match the username and password of the outgoing authentication account of the headquarters' ZyXEL Device. This can be configured in the **VoIP > Trunking > Peer Call** screen.

Figure 166 VoIP to PSTN Example - Incoming Authentication



13.8.4 Call Progression

The advantage of this kind of VoIP trunking is that once all the configuration is completed, the caller just has to dial a speed dial entry from a phone connected to their ZyXEL Device and the peer devices take care of the rest. This is what happens when headquarters wants to call their **Sales1** employee, which is the first entry in the speed dial screen.

Table 76 VoIP Trunking Call Progression

HEADQUARTERS	BRANCH OFFICE	SALES1
A person at **A** dials #01 from the phone connected to the ZyXEL Device.		
The ZyXEL Device at **A** inspects the number and connects to the remote peer device at **B**. →		
The remote peer device inspects the number and requests authentication in order to forward the call. ←		
The ZyXEL Device at **A** sends outgoing authentication to the remote peer device. →		
The remote peer device confirms that the username and password match an account in its incoming authentication list. ←		
	The remote peer device forwards the call to **Sales1**. →	
Sales1 picks up and the call commences. ↔		

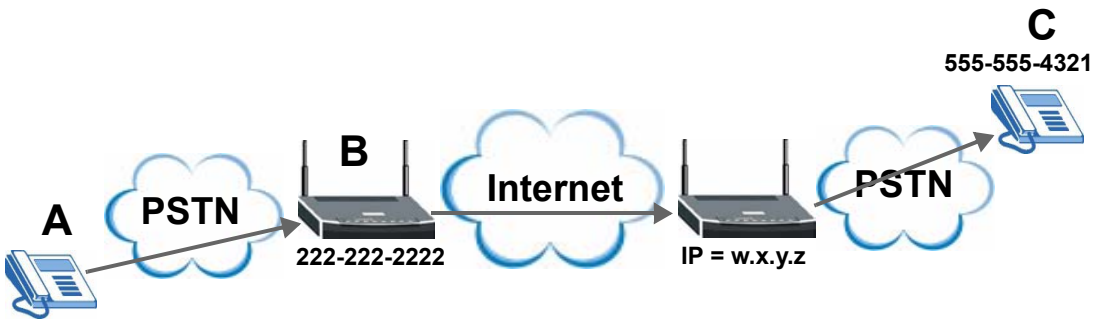
13.9 VoIP Trunking Example: PSTN to PSTN via VoIP

This example shows how to configure a PSTN to PSTN call with a VoIP link. It also shows how call rules can be used to automate VoIP trunking.

13.9.1 Background Information

A company has its headquarters in two different cities. The sales manager (**A**) from headquarters often needs to call salespeople (**D**) employed at the branch office. The sales manager often works away from the headquarters office and the sales employees often work away from the branch office. The sales manager and the sales employees have PSTN phones (mobile or land based). The two offices have VoIP trunking devices. The sales manager wants to use VoIP trunking to save on calls to his sales team. The head office has a ZyXEL Device (**B**) with a PSTN line (tel: 222-222-2222) connected to it. The branch office has a ZyXEL Device (**C**) with a public IP address **w.x.y.z**. The sales employee (**D**) has a PSTN phone with the number 555-555-4321.

Figure 167 PSTN to PSTN Example



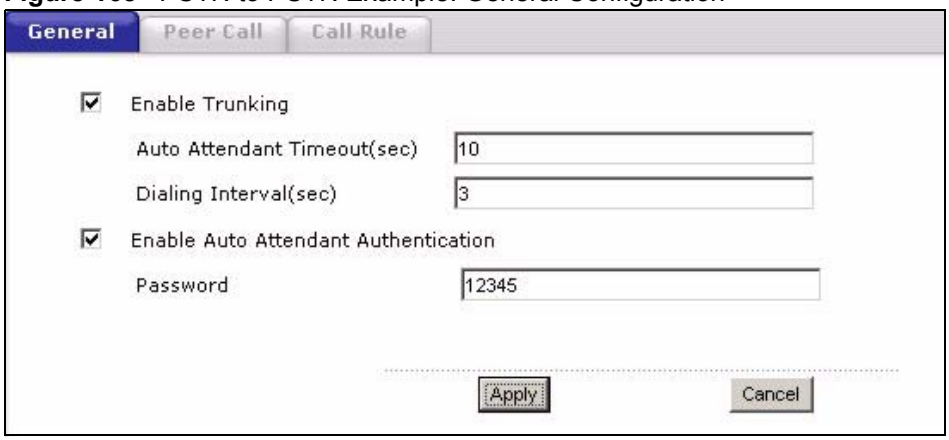
The proposed solution is to configure a call rule which will allow the sales manager to call into the headquarters via PSTN, establish a VoIP link between the two ZyXEL Devices and have the remote peer device forward calls to the sales employees via PSTN.

13.9.2 Configuration Details: Outgoing

The ZyXEL Device (at headquarters) from which the VoIP link originates needs to have the following configuration settings:

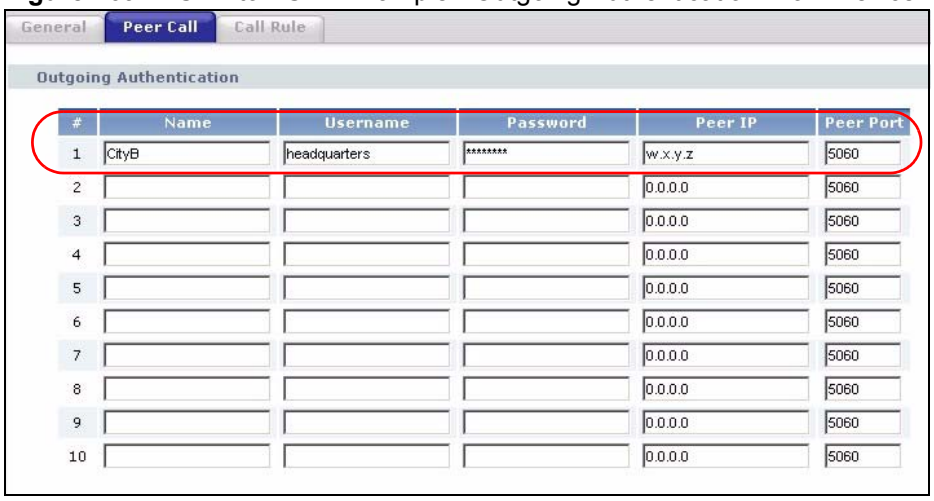
1. Auto attendant authentication needs to be enabled for PSTN calls coming into the headquarters' ZyXEL Device. This ensures that no unauthorized callers use VoIP trunking. In this example the PIN (Personal Identification Number) is set to "12345"**.** The settings dealing with dialing interval and a timeout period are left at default. The ZyXEL Device waits 10 seconds (after initial connection between PSTN caller and the ZyXEL Device) for the PSTN caller to initiate VoIP trunking by dialing another number. It waits 3 seconds between dialing digits before it determines that the entire phone number is entered. These settings can be configured in the **VoIP > Trunking > General** screen.

Figure 168 PSTN to PSTN Example: General Configuration



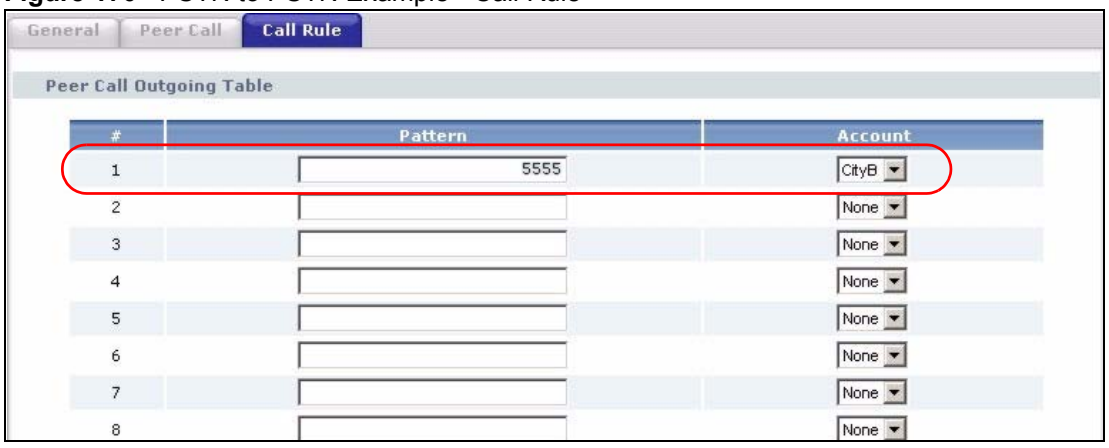
2 An outgoing authentication account needs to be configured. This account consists of the IP address and port number of the branch office ZyXEL Device as well as the username and password for authentication. This username and password must match the incoming authentication account username and password on the branch office ZyXEL Device. The name of this account is "CityB" referring to the branch office ZyXEL Device. In this example the username is "headquarters" and the password is "password". This can be configured in the **VoIP** > **Trunking** > **Peer Call** screen.

Figure 169 PSTN to PSTN Example - Outgoing Authentication From Device B



3 A call rule needs to be created. This rule tells the ZyXEL Device which remote peer device it should connect to in order to complete the call. This rule is composed of a pattern and an account name. This pattern is simply the first several digits of the number you want the remote device to connect to. In this example this is the first 4 digits ("5555") of "Sales1" telephone number. The account name is the name of the outgoing authentication account created in the **Speed Dial** screen ("CityB"). This setting can be configured in the **VoIP > Trunking > Call Rule** screen.

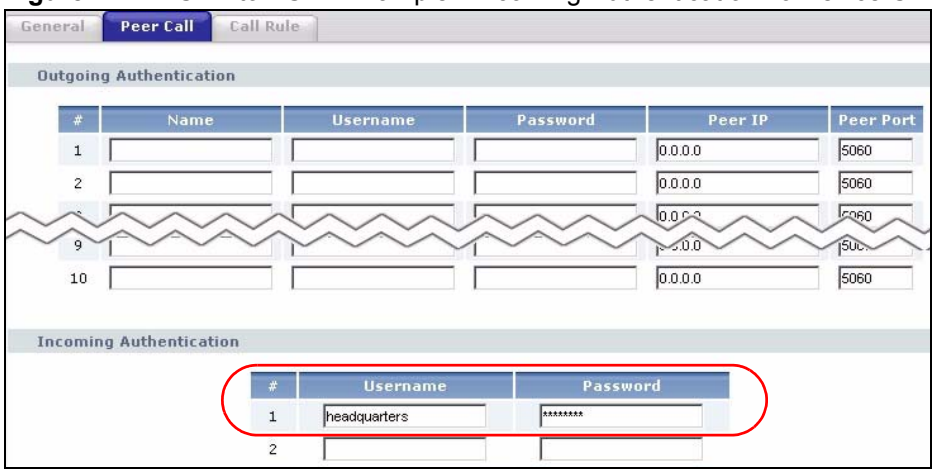
Figure 170 PSTN to PSTN Example - Call Rule



13.9.3 Configuration Details: Incoming

The branch office ZyXEL Device needs to have an incoming authentication account configured. This consists of a username and password. This account must match the username and password of the outgoing authentication account of the headquarters' ZyXEL Device. This can be configured in the **VoIP > Trunking > Peer Call** screen.

Figure 171 PSTN to PSTN Example - Incoming Authentication To Device C



13.9.4 Call Progression

The call is initiated by the manager dialing into the headquarter's ZyXEL Device via PSTN. In this scenario a VoIP link is established between headquarters and the branch office and then the call is forwarded to **Sales1** using PSTN.

Table 77 PSTN to PSTN: VoIP Trunking Call Progression

MANAGER	HEADQUARTERS	BRANCH OFFICE	SALES1
The manager dials the PSTN number of the headquarters' ZyXEL Device. (**222-222-2222**)			
The ZyXEL Device receives the call and sends a ringback alert tone to indicate to the caller that VoIP trunking is enabled.			
The manager dials the PSTN number of **Sales1** (**555-555-1234**).			
The ZyXEL Device prompts the manager to enter the PIN in order to allow VoIP trunking.			
The manager dials the PIN (**12345**).			
	The ZyXEL Device confirms the password and allows for VoIP trunking. The ZyXEL Device inspects the phone number against call rules. Since the number starts with the pattern (**5555**), it uses the account (**CityB**) associated with this pattern to connect the call to the remote peer device at the branch office.		
	The remote peer device inspects the number and requests authentication in order to forward the call.		
	The ZyXEL Device at **A** sends outgoing authentication to the remote peer device.		
	The remote peer device confirms that the username and password match an account in its incoming authentication list.		
		The remote peer device forwards the call to **Sales1**.	
Sales1 picks up and the call commences.			

14

Phone Usage

This chapter describes how to use a phone connected to your ZyXEL Device for basic tasks.

Not all service providers support all features.

14.1 Dialing a Telephone Number

The **PHONE** LED turns green when your SIP account is registered. Dial a SIP number like "12345" on your phone's keypad.

Use speed dial entries (see Section 12.14 on page 213) for peer-to-peer calls or SIP numbers that use letters. Dial the speed dial entry on your telephone's keypad.

Use your VoIP service provider's dialing plan to call regular telephone numbers.

14.2 Using Speed Dial to Dial a Telephone Number

After configuring the speed dial entry and adding it to the phonebook, press the speed dial entry's key combination on your phone's keypad.

14.3 Internal Calls

Press "####" on your phone's keypad to call the ZyXEL Device's other phone port.

14.4 Using Call Park and Pickup

Do the following to put a call on hold on one phone and continue it on another (connected to the ZyXEL Device). This feature may not be supported by all service providers.

1. During the call, press "*97#" and then any number (up to 8 digits long). You need to remember this number in order to pick up the call on another phone. Hang up the receiver.
2. Pick up another phone's receiver. Press "#97#" followed by the same number you entered before to continue the call.

14.5 Checking the ZyXEL Device's IP Address

Do the following to listen to the ZyXEL Device's current IP address.

1. Pick up your phone's receiver.
2. Press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
3. Press "5" followed by the # key.
4. Listen to the IP address and make a note of it.
5. Hang up the receiver.

14.6 Auto Provisioning and Auto Firmware Upgrade

If your service provider uses an auto-provisioning server to set up your device, you must first enter the HTTP pincode (supplied by your service provider). This authenticates your ZyXEL Device with the auto provisioning server, allowing you to use the service.

- On a phone connected to the device, enter "*99**", your SIP number, "*", the HTTP pincode you were given, then "#".
- For example, if your SIP number is 0123456 and the HTTP pincode you were given is 9876, you would enter "*99**0123456*9876#".

During auto-provisioning, the ZyXEL Device checks to see if there is a newer firmware version (if your service provider activates this feature). If newer firmware is available, the ZyXEL Device plays a recording when you pick up your phone's handset.

- Press "*99#" to upgrade the ZyXEL Device's firmware.
- Press "#99#" to not upgrade the ZyXEL Device's firmware.

14.7 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 78 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
****	IVR	Use this to set up Interactive Voice Response. IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold). See Section 12.2.10 on page 191.
####	Internal call	Call the phone(s) connected to the ZyXEL Device. See Chapter 32 on page 433.
*99**	HTTP pincode	Use this if your service provider gave you a personal identification number to enter in order to start using the service. See Section 14.6 on page 238.
*99#	Enable firmware update	Use these to upload or not upload new firmware to the ZyXEL Device, if requested by your service provider. See Section 14.6 on page 238.
#99#	Disable firmware update	

Table 78 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 12.12.2 on page 209 (Europe type) and Section 12.12.3 on page 211 (USA type).
*97#	Call park	Use these to place a call on hold on one phone and then continue it on another (if supported by your service provider). See Chapter 32 on page 433.
#97#	Call pickup	
*66#	Call return	Place a call to the last person who called you. See Chapter 32 on page 433.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off. Chapter 32 on page 433
#95#	Disable Do Not Disturb	
*41#	Enable call waiting	Use these to allow you to put a call on hold while answering another, or to turn this function off. See Section 12.12.2 on page 209 (Europe type) and Section 12.12.3 on page 211 (USA type).
#41#	Disable call waiting	
*21#	Enable call forward	Use these to allow you to use the call forwarding tables you set in the ZyXEL Device, or to turn this function off. See Section 12.15 on page 214.
#21#	Disable call forward	
22	Uncondition forward	Forward all incoming calls. See Section 12.15 on page 214.
23	No answer forward	Forward incoming calls if you do not answer. See Section 12.15 on page 214.
24	Busy forward	Forward calls if you are already making a call. See Section 12.15 on page 214.
*67	One shot caller ID hide	Activate or deactivate caller ID for the next call only. See Section 12.4 on page 193.
*82	One shot caller ID display	
*70	One shot Call Waiting Disable	Activate or deactivate call waiting on the next call only. See Section 12.12.2 on page 209 (Europe type) and Section 12.12.3 on page 211 (USA type)
*85	One shot Call Waiting Enable	

15

Firewalls

Use these screens to enable and configure the firewall that protects your ZyXEL Device and your LAN from unwanted or malicious traffic.

15.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

15.1.1 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

15.1.2 About the ZyXEL Device Firewall

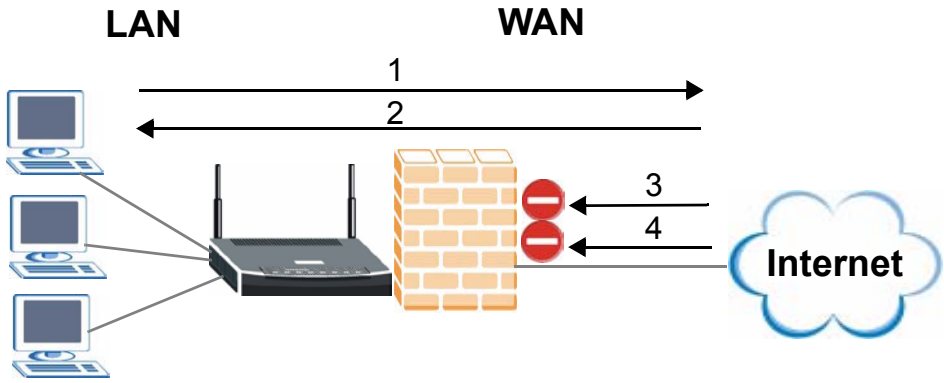
The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The ZyXEL Device is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

Figure 172 Default Firewall Action



Your customized rules take precedence and override the ZyXEL Device's default settings. The ZyXEL Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyXEL Device takes the action specified in the rule.

15.1.3 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

15.2 General Firewall Policy Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- LAN to WAN
- WAN to LAN
- WAN to WAN/ Router

The LAN includes both the LAN port and the WLAN.

By default, the ZyXEL Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router
  These rules specify which computers on the LAN can manage the ZyXEL Device (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

You can also configure the remote management settings to allow only a specific computer to manage the ZyXEL Device.

- LAN to WAN
  These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the ZyXEL Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN
  These rules specify which computers on the WAN can access which computers or services on the LAN.

You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to WAN/ Router
  By default the ZyXEL Device stops computers on the WAN from managing the ZyXEL Device or using the ZyXEL Device as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyXEL Device.

You also need to configure the remote management settings to allow a WAN computer to manage the ZyXEL Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.

- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL Device's default rules.

15.3 Security Considerations

Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyXEL Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

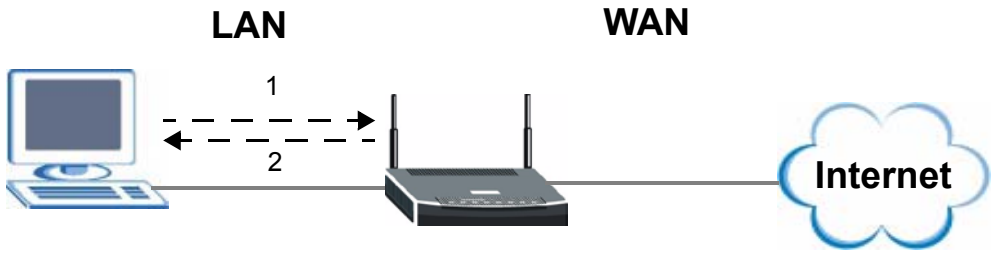
1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens..

15.4 Triangle Route

When the firewall is on, your ZyXEL Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyXEL Device to protect your LAN against attacks.

Figure 173 Ideal Firewall Setup



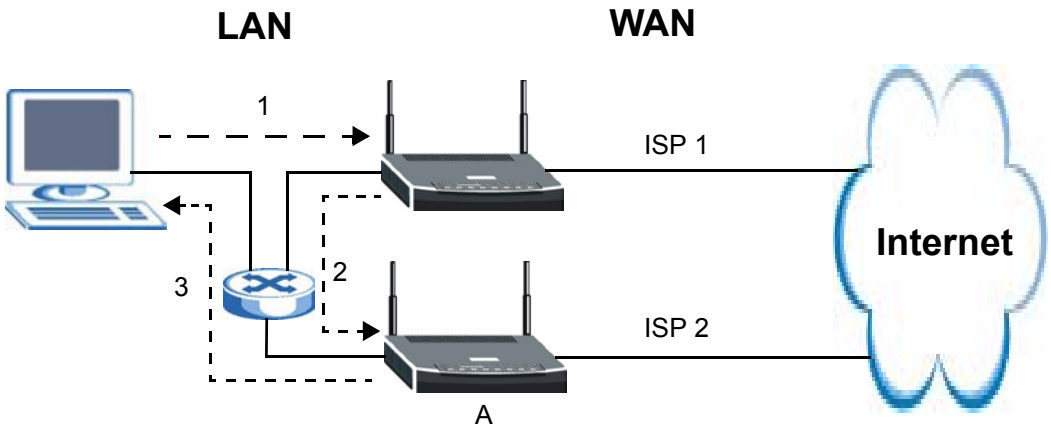
15.4.1 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the ZyXEL Device’s LAN IP address), the “triangle route” (also called asymmetrical route) problem may occur. The steps below describe the “triangle route” problem.

1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
2. The ZyXEL Device reroutes the SYN packet through Gateway **A** on the LAN to the WAN.
3. The reply from the WAN goes directly to the computer on the LAN without going through the ZyXEL Device.

As a result, the ZyXEL Device resets the connection, as the connection has not been acknowledged.

Figure 174 “Triangle Route” Problem



15.4.2 Solving the “Triangle Route” Problem

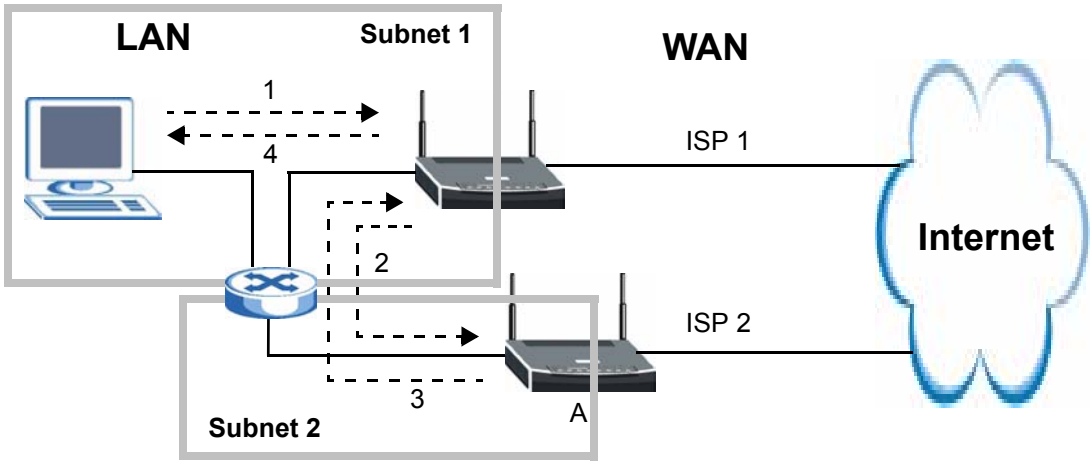
If you have the ZyXEL Device allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the ZyXEL Device and its firewall protection.

Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network.

It’s like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyXEL Device reroutes the packet to Gateway A, which is in Subnet 2.
3. The reply from the WAN goes to the ZyXEL Device.
4. The ZyXEL Device then sends it to the computer on the LAN in Subnet 1.

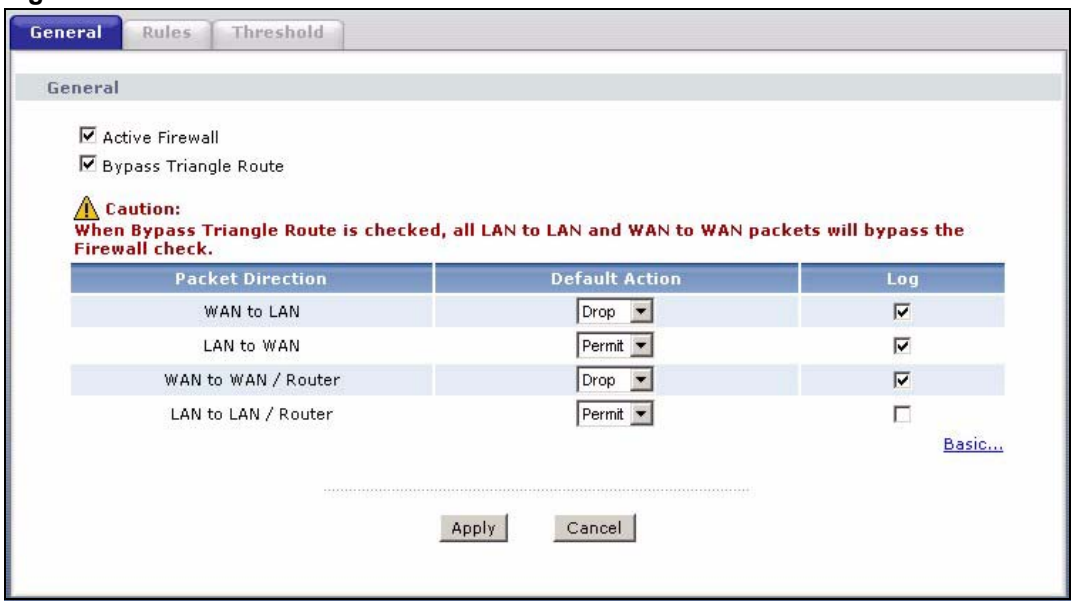
Figure 175 IP Alias



15.5 General Firewall Policy

Click **Security > Firewall** to display the following screen. Activate the firewall by selecting the **Active Firewall** check box as seen in the following screen.

Figure 176 Firewall: General



The following table describes the labels in this screen.

Table 79 Firewall: General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ZyXEL Device's LAN IP address, return traffic may not go through the ZyXEL Device. This is called an asymmetrical or "triangle" route. This causes the ZyXEL Device to reset the connection, as the connection has not been acknowledged. Select this check box to have the ZyXEL Device permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyXEL Device. A better solution is to use IP alias to put the ZyXEL Device and the backup gateway on separate subnets. See Section 15.4.1 on page 245 for an example.
Packet Direction	This is the direction of travel of packets (**LAN to LAN / Router**, **LAN to WAN**, **WAN to WAN / Router**, **WAN to LAN**). Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, **LAN to LAN / Router** means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself.
Default Action	Use the drop-down list boxes to select the default action that the firewall is take on packets that are traveling in the selected direction and do not match any of the firewall rules. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

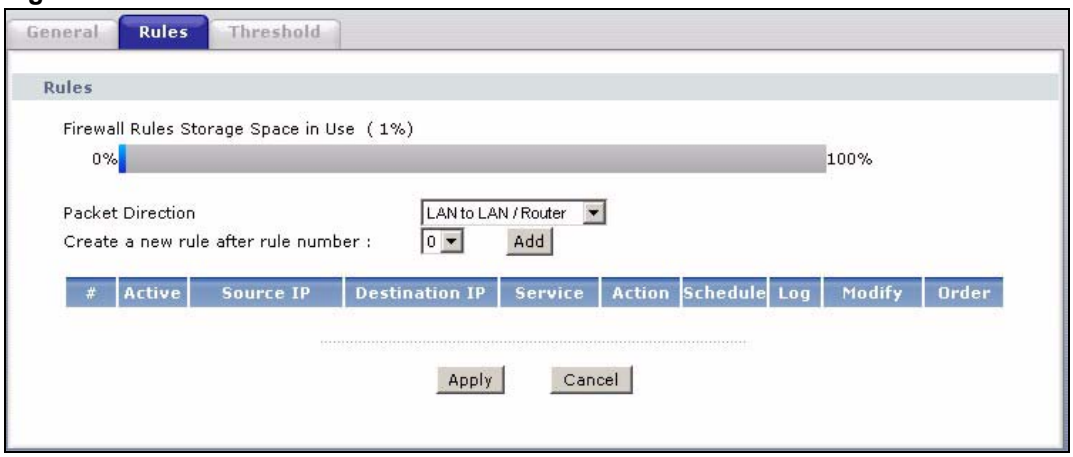
15.6 Firewall Rules Summary

The ordering of your rules is very important as rules are applied in turn.

Refer to Section 15.2 on page 242 for more information.

Click **Security > Firewall > Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

Figure 177 Firewall Rules



The following table describes the labels in this screen.

Table 80 Firewall Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click **Add** to add a new firewall rule after the selected index number. For example, if you select “6”, your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the **General** screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service	This drop-down list box displays the services to which this firewall rule applies. See Appendix E on page 499 for more information.
Action	This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Schedule	This field tells you whether a schedule is specified (**Yes**) or not (**No**).
Log	This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**).

Table 80 Firewall Rules (continued)

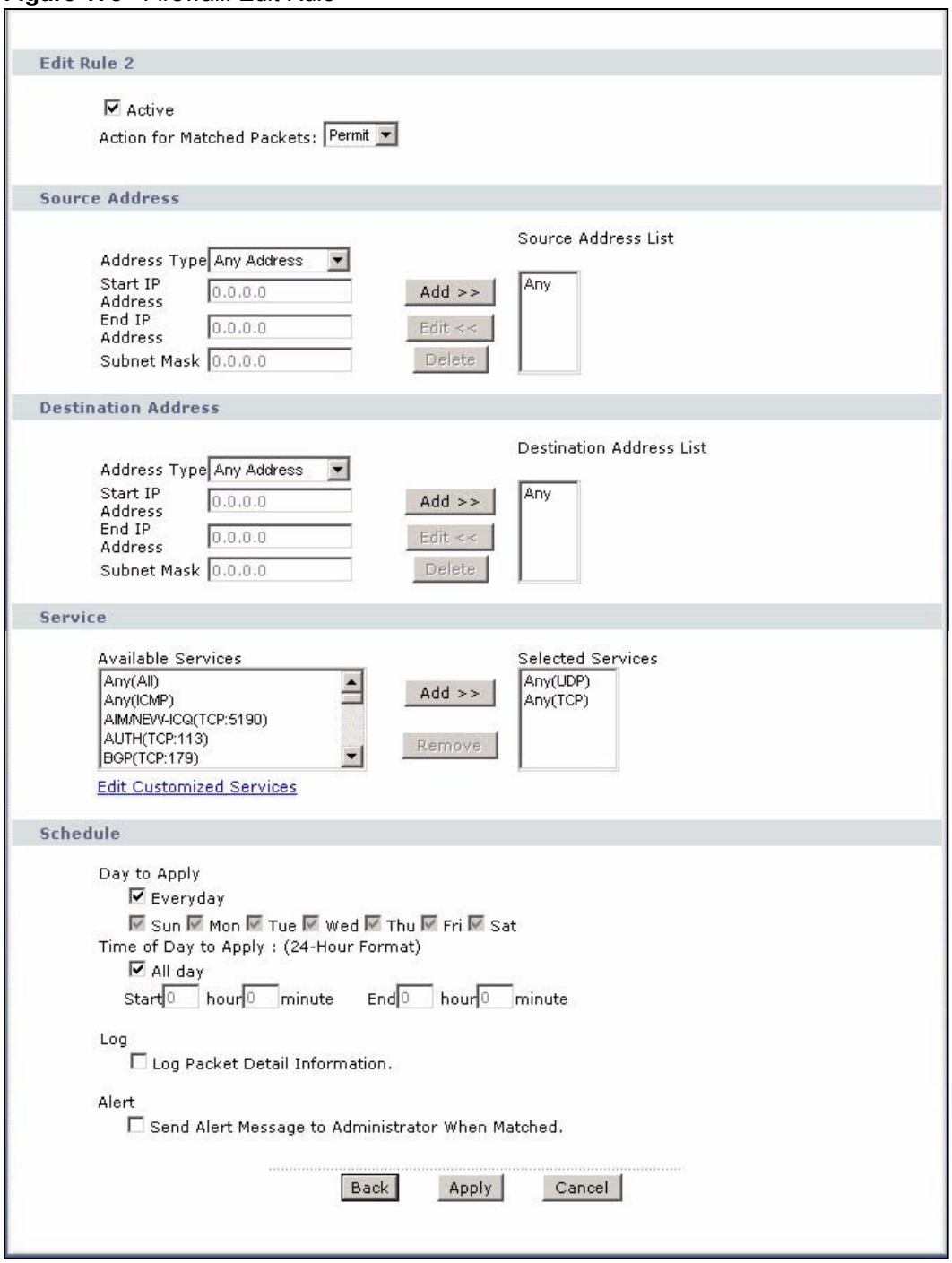
LABEL	DESCRIPTION
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the **Move the rule to** field. Type a number in the **Move the rule to** field and click the **Move** button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.6.1 Configuring Firewall Rules

Refer to Section 15.2 on page 242 for more information.

In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 178 Firewall: Edit Rule



The following table describes the labels in this screen.

Table 81 Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender of (**Reject**) or allow the passage of (**Permit**) packets that match this rule.

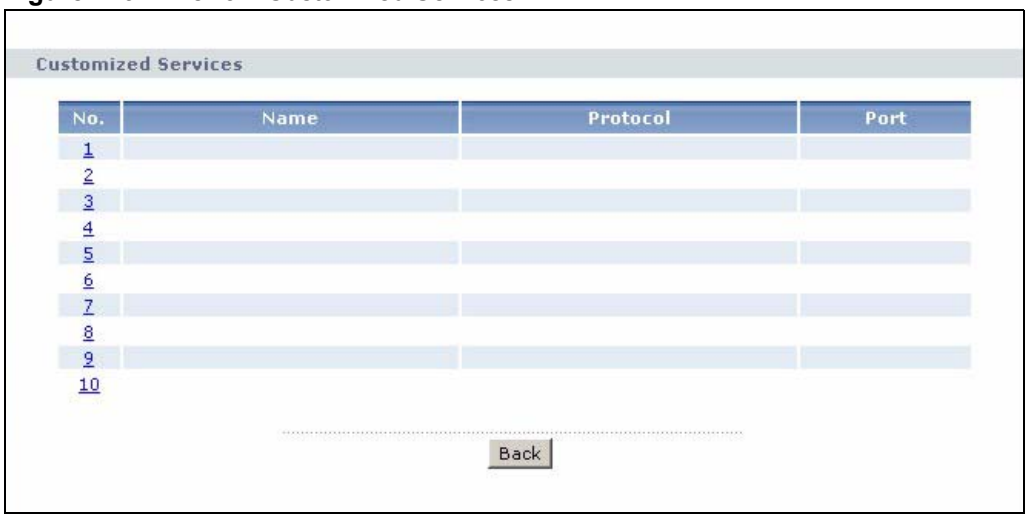
Table 81 Firewall: Edit Rule (continued)

LABEL	DESCRIPTION
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click **Add >>** to add a new address to the **Source** or **Destination Address** box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click **Edit <<**.
Delete	Highlight an existing source or destination address from the **Source** or **Destination Address** box above and click **Delete** to remove it.
Services	
Available/ Selected Services	Please see Appendix E on page 499 for more information on services available. Highlight a service from the **Available Services** box on the left, then click **Add >>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **Remove**.
Edit Customized Service	Click the **Edit Customized Services** link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyXEL Device record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

15.6.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix E on page 499 for some examples. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Figure 179 Firewall: Customized Services



The following table describes the labels in this screen.

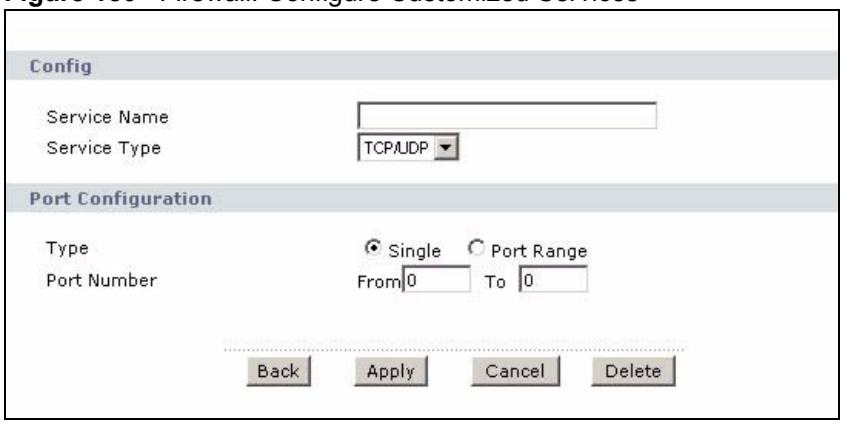
Table 82 Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the **Firewall Customized Services Config** screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP**, **UDP** or **TCP/UDP**) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click **Back** to return to the **Firewall Edit Rule** screen.

15.6.3 Configuring A Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Figure 180 Firewall: Configure Customized Services



The following table describes the labels in this screen.

Table 83 Firewall: Configure Customized Services

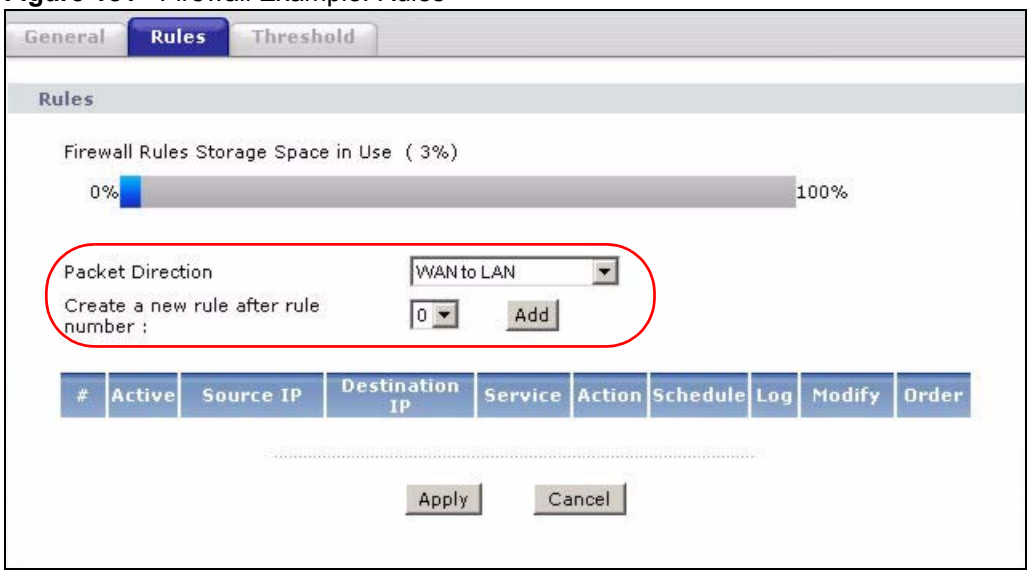
LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to delete the current rule.

15.7 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical “MyService” connection from the Internet.

1. Click **Security > Firewall** > **Rules**.
2. Select **WAN to LAN** in the **Packet Direction** field.

Figure 181 Firewall Example: Rules



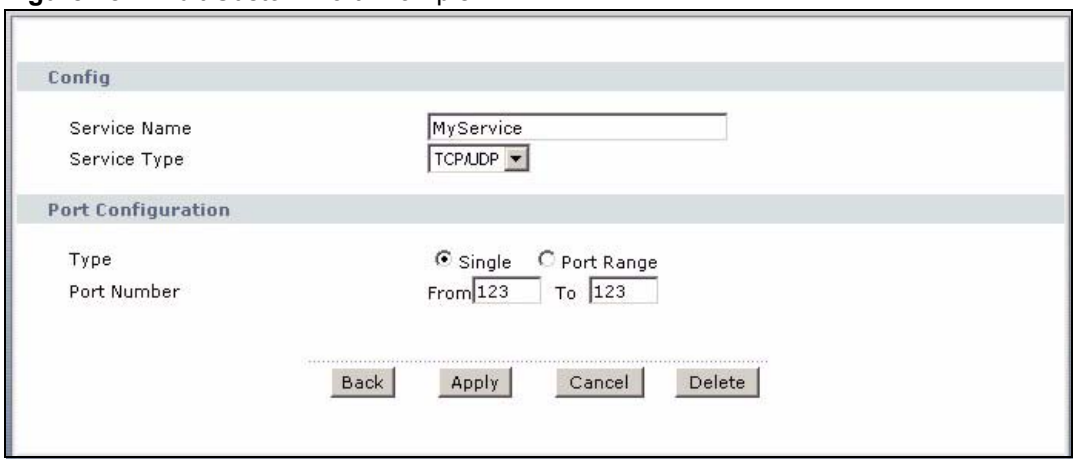
3 In the **Rules** screen, select the index number after that you want to add the rule. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.

4 Click **Add** to display the firewall rule configuration screen.

5 In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.

6 Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

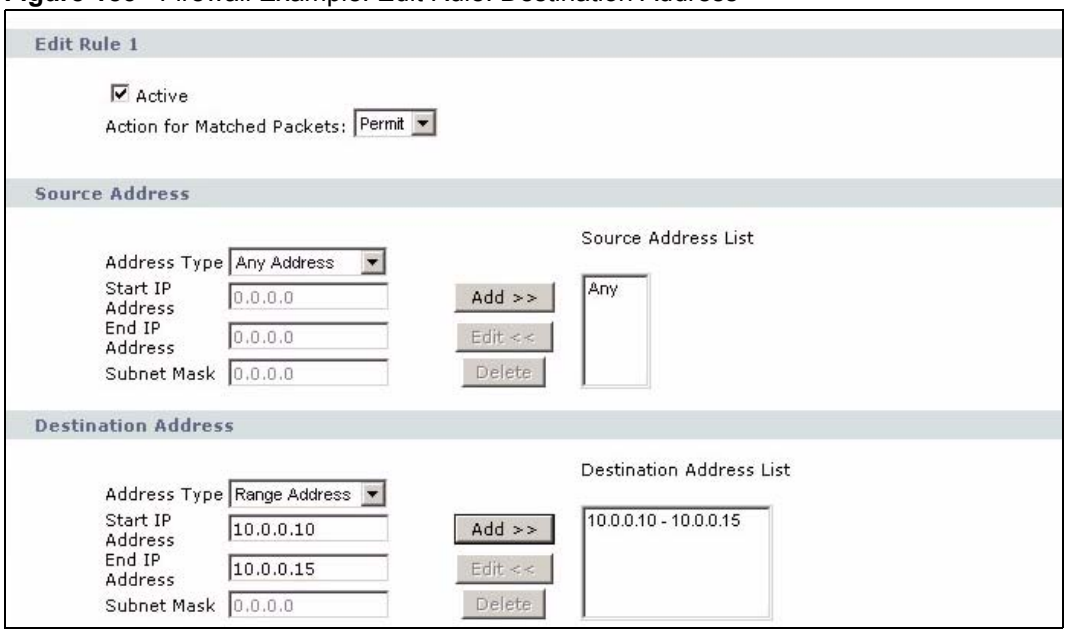
Figure 182 Edit Custom Port Example



7 Select **Any** in the **Destination Address List** box and then click **Delete**.

8 Configure the destination address screen as follows and click **Add**.

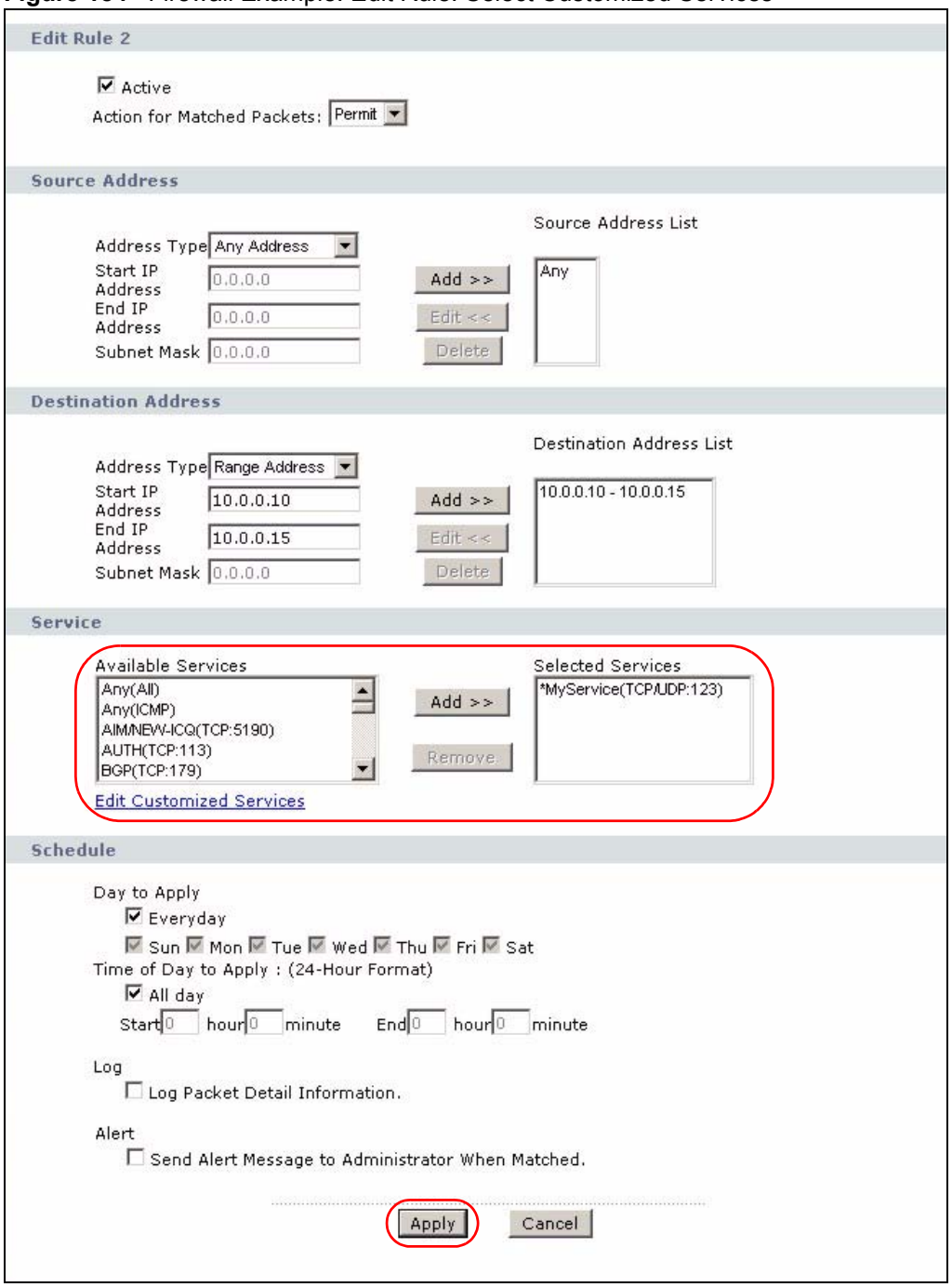
Figure 183 Firewall Example: Edit Rule: Destination Address



9 Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

Custom services show up with an "*" before their names in the **Services** list box and the **Rules** list box.

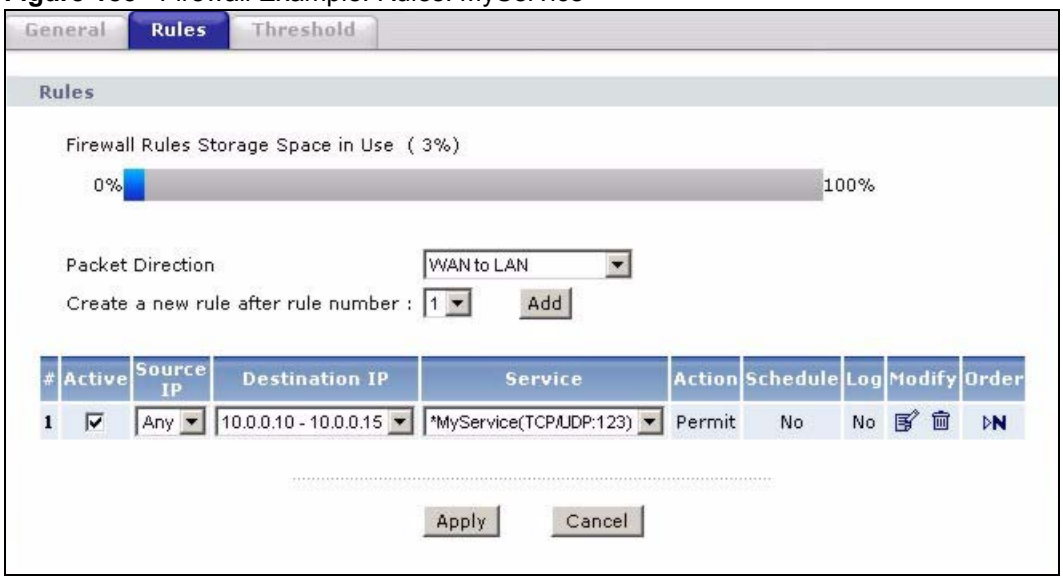
Figure 184 Firewall Example: Edit Rule: Select Customized Services



On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

Rule 1 allows a “MyService” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Figure 185 Firewall Example: Rules: MyService

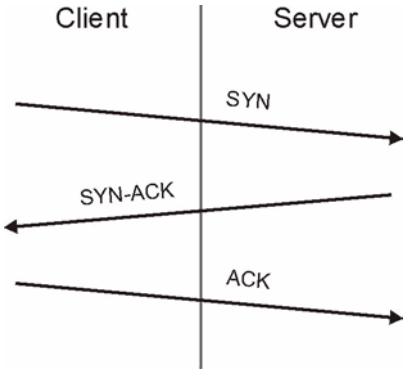


15.8 Firewall Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 186 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

15.8.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyXEL Device has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyXEL Device is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.
2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

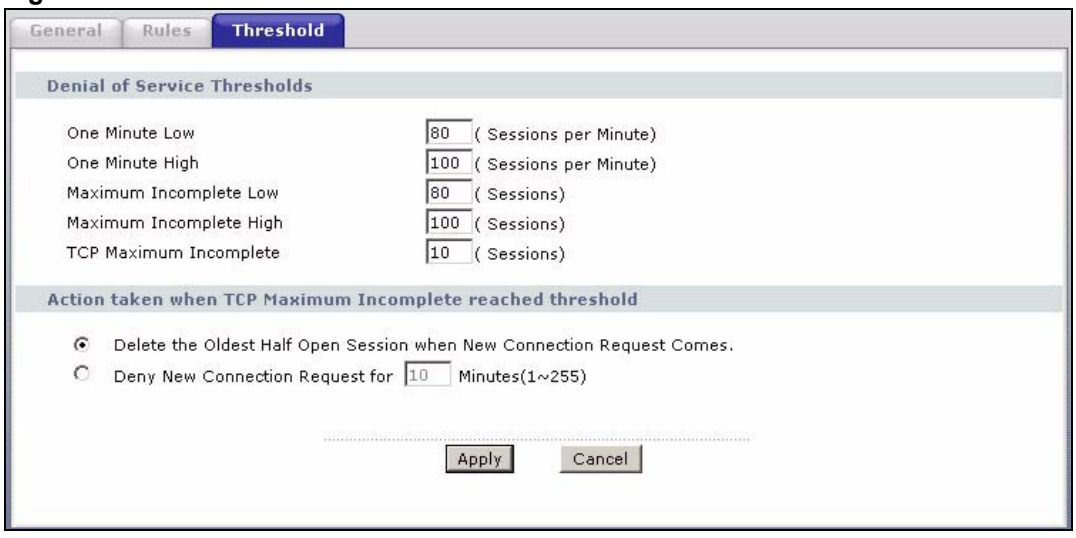
- If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyXEL Device may classify them as DoS attacks.

15.8.2 Configuring Firewall Thresholds

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall** > **Threshold** to bring up the next screen.

Figure 187 Firewall: Threshold



The following table describes the labels in this screen.

Table 84 Firewall: Threshold

LABEL	DESCRIPTION
Denial of Service Thresholds	The ZyXEL Device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts. For example, if you set the one minute high to 100, the ZyXEL Device starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. For example, if you set the maximum incomplete high to 100, the ZyXEL Device starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.
TCP Maximum Incomplete	An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host. Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The ZyXEL Device sends alerts whenever the **TCP Maximum Incomplete** is exceeded.
Action taken when TCP Maximum Incomplete reached threshold	Select the action that ZyXEL Device should take when the TCP maximum incomplete threshold is reached. You can have the ZyXEL Device either: Delete the oldest half open session when a new connection request comes. or Deny new connection requests for the number of minutes that you specify (between 1 and 255).
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.

16

Content Filtering

This chapter covers how to configure content filtering.

16.1 Content Filtering Overview

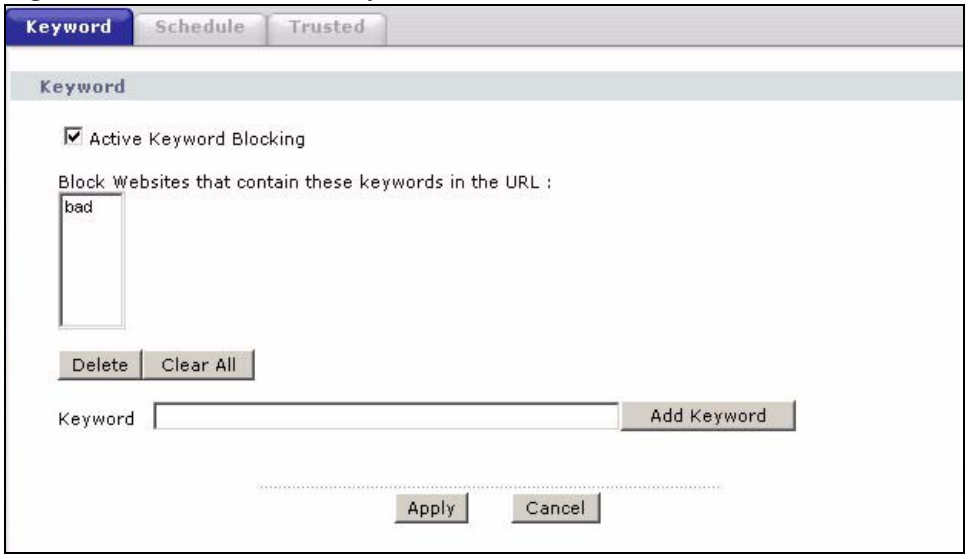
Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for when the ZyXEL Device performs content filtering. You can also specify trusted IP addresses on the LAN for which the ZyXEL Device will not perform content filtering.

16.2 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the ZyXEL Device blocks all sites containing this keyword including the URL http://www.website.com/bad.html, even if it is not included in the Filter List.

To have your ZyXEL Device block Web sites containing keywords in their URLs, click **Security > Content Filter**. The screen appears as shown.

Figure 188 Content Filter: Keyword



The following table describes the labels in this screen.

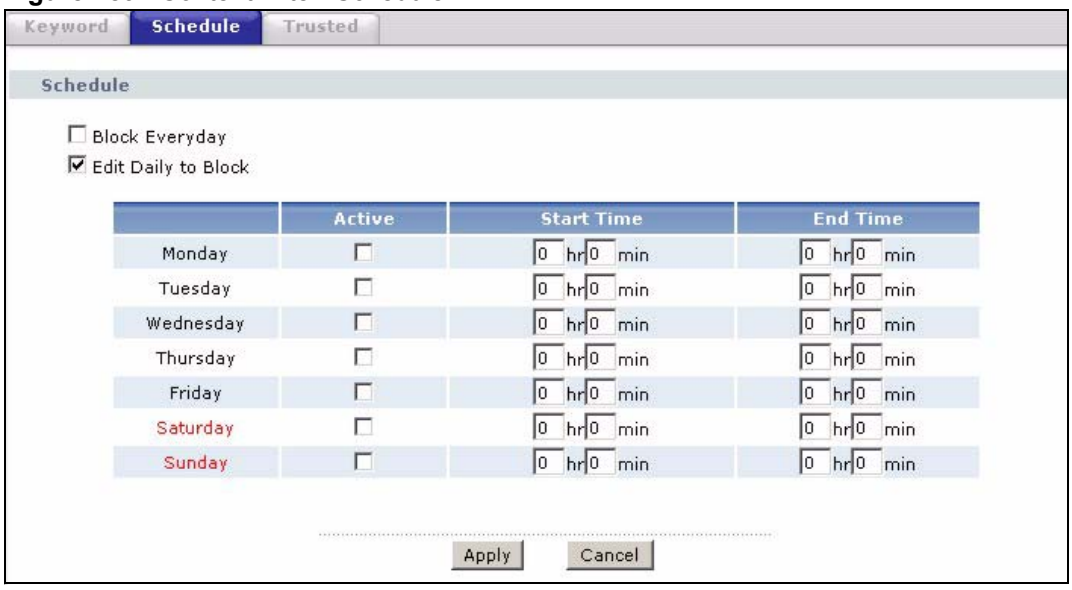
Table 85 Content Filter: Keyword

LABEL	DESCRIPTION
Active Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the ZyXEL Device to block.
Delete	Highlight a keyword in the box and click **Delete** to remove it.
Clear All	Click **Clear All** to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click **Add Keyword** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previously saved settings.

16.3 Configuring the Schedule

Use this screen to set the days and times for the ZyXEL Device to perform content filtering. Click **Security > Content Filter** > **Schedule**. The screen appears as shown.

Figure 189 Content Filter: Schedule



The following table describes the labels in this screen.

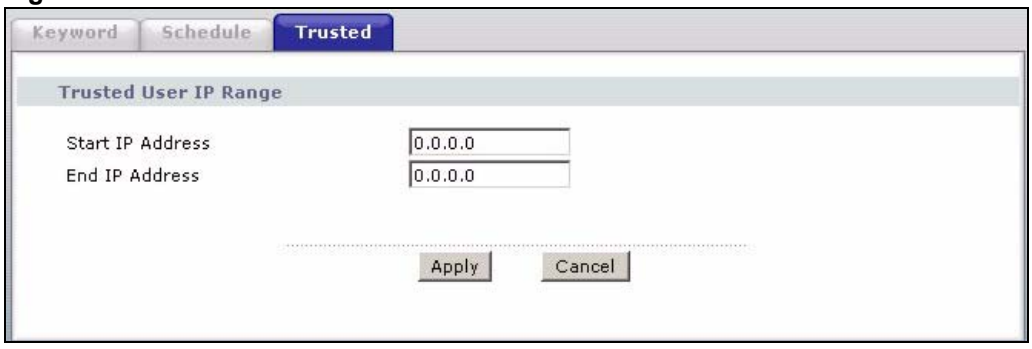
Table 86 Content Filter: Schedule

LABEL	DESCRIPTION
Schedule	Select **Block Everyday** to make the content filtering active everyday. Otherwise, select **Edit Daily to Block** and configure which days of the week (or everyday) and which time of the day you want the content filtering to be active.
Active	Select the check box to have the content filtering to be active on the selected day.
Start TIme	Enter the time when you want the content filtering to take effect in hour-minute format.
End Time	Enter the time when you want the content filtering to stop in hour-minute format.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previously saved settings.

16.4 Configuring Trusted Computers

Use this screen to exclude a range of users on the LAN from content filtering on your ZyXEL Device. Click **Security > Content Filter** > **Trusted**. The screen appears as shown.

Figure 190 Content Filter: Trusted



The following table describes the labels in this screen.

Table 87 Content Filter: Trusted

LABEL	DESCRIPTION
Trusted User IP Range	
Start IP Address	Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.
End IP Address	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previously saved settings.

17

Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

17.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

17.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

17.1.2 Security Association

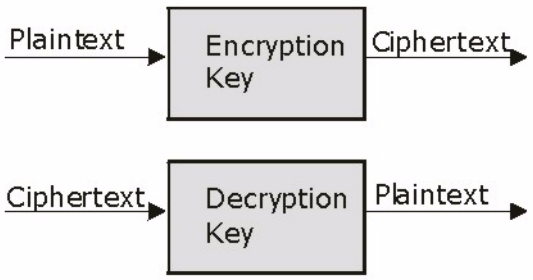
A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

17.1.3 Other Terminology

17.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

Figure 191 Encryption and Decryption



17.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

17.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

17.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

17.1.4 VPN Applications

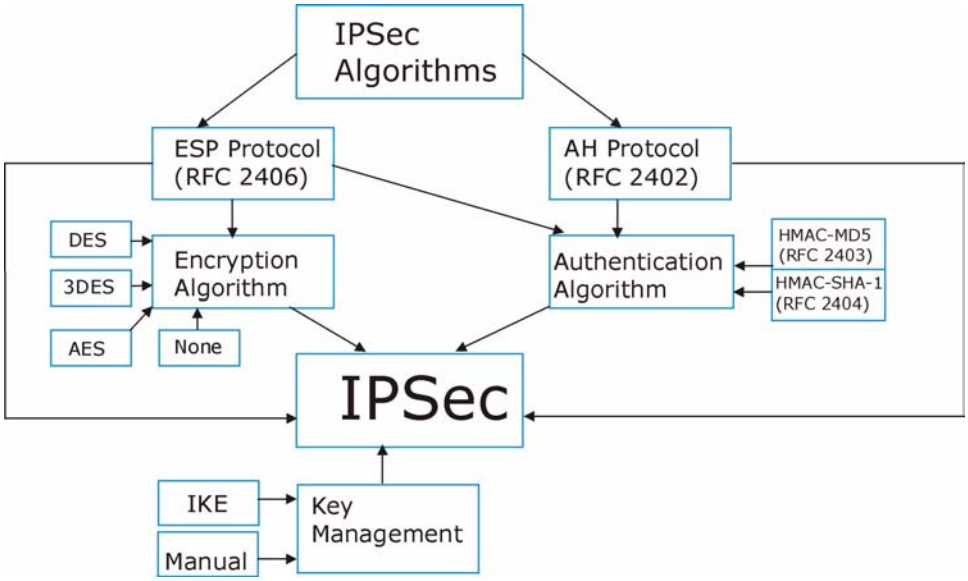
The ZyXEL Device supports the following VPN applications.

- Linking Two or More Private Networks Together
  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.
- Accessing Network Resources When NAT Is Enabled
  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.
- Unsupported IP Applications
  A VPN tunnel may be created to add support for unsupported emerging IP applications.

17.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 192 IPSec Architecture



17.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please seeSection 18.2 on page 271for more information.

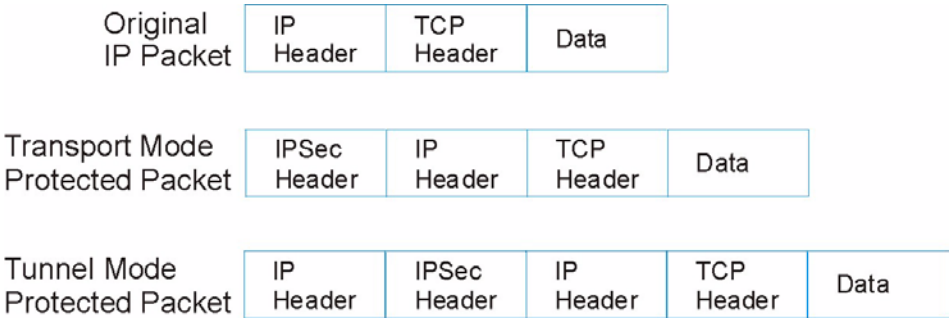
17.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

17.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 193 Transport and Tunnel Mode IPSec Encapsulation



17.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

17.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

17.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyXEL Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 88 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

18

VPN Screens

This chapter introduces the VPN screens. See Chapter 28 on page 395 for information on viewing logs and the appendix for IPSec log descriptions.

18.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

18.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

18.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

18.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 89 AH and ESP

	ESP	AH
ENCRYPTION		
	DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	
AUTHENTICATION	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA1** for maximum security.	

18.3 My IP Address

My IP Address is the WAN IP address of the ZyXEL Device. The ZyXEL Device has to rebuild the VPN tunnel if My IP Address changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See Chapter 8 on page 127 for details on dial backup and traffic redirect.

18.4 Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyXEL Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

18.4.1 Dynamic Secure Gateway Address

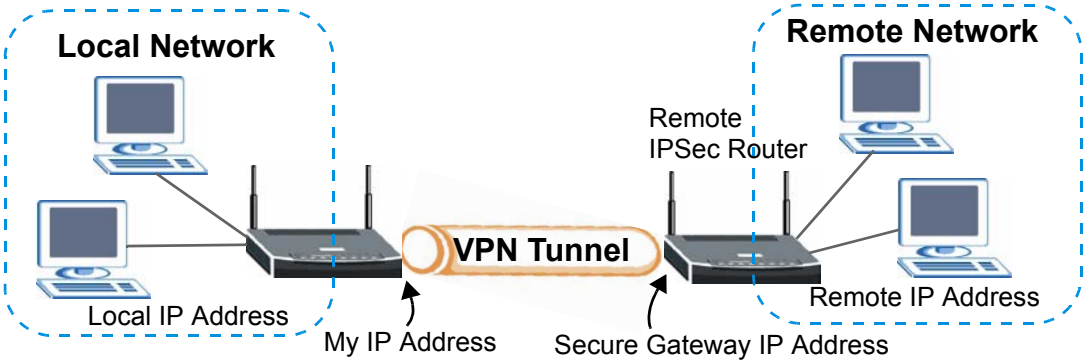
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (seeSection 18.18 on page 293for configuration examples).

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using **IKE** key management and not **Manual** key management.

18.5 VPN Setup Screen

The following figure helps explain the main fields in the web configurator.

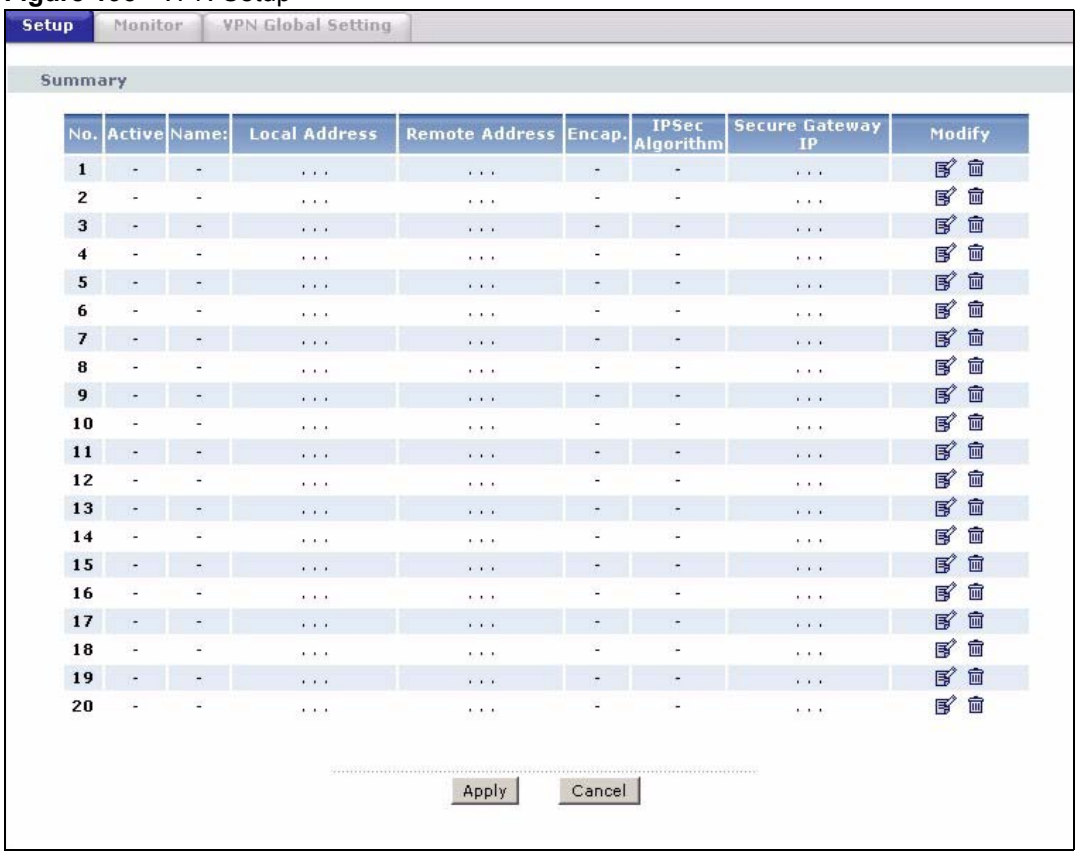
Figure 194 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security** > **VPN** to open the **VPN Setup** screen. This is a menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

Figure 195 VPN Setup



The following table describes the fields in this screen.

Table 90 VPN Setup

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Name	This field displays the identification name for this VPN policy.
Local Address	This is the IP address(es) of computer(s) on your local network behind your ZyXEL Device. The same (static) IP address is displayed twice when the **Local Address Type** field in the **VPN Setup - Edit** screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **VPN Setup - Edit** screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **VPN Setup - Edit** screen is configured to **Subnet**.

Table 90 VPN Setup

LABEL	DESCRIPTION
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Address Type** field in the **VPN Setup - Edit** screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **VPN Setup - Edit** screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **VPN Setup - Edit** screen is configured to **Subnet**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase ZyXEL Device processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **VPN-IKE** screen to **0.0.0.0.**
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN configuration. Click the **Remove** icon to remove an existing VPN configuration.
Apply	Click this to save your changes and apply them to the ZyXEL Device.
Cancel	Click this return your settings to their last saved values.

18.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL Device automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see Section 18.12 on page 284 for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a ZyXEL Device-compatible keep alive feature enabled in order for this feature to work.

If the ZyXEL Device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL Device because the ZyXEL Device never drops the tunnels that are already connected.

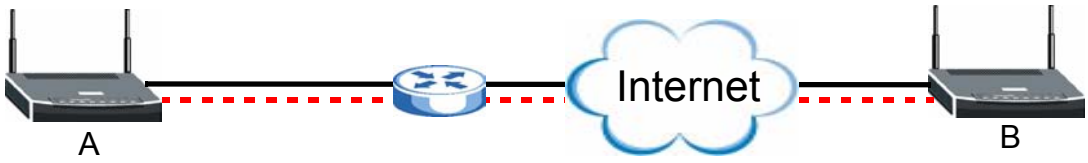
When there is outbound traffic with no inbound traffic, the ZyXEL Device automatically drops the tunnel after two minutes.

18.7 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the ZyXEL Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 196 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In Figure 196 on page 276, when IPSec router A tries to establish an IKE SA, IPSec router B checks the UDP port 500 header, and IPSec routers A and B build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router A.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 91 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

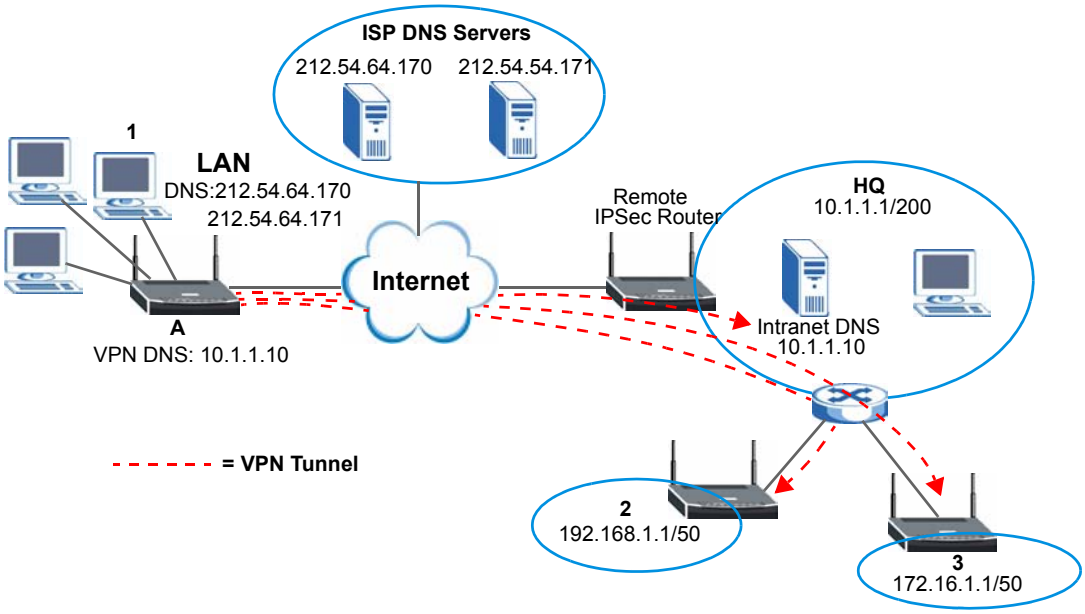
Y* - This is supported in the ZyXEL Device if you enable NAT traversal.

18.8 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network

The following figure depicts an example where three VPN tunnels are created from ZyXEL Device A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the ZyXEL Device at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 197 VPN Host using Intranet DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

18.9 ID Type and Content

With aggressive negotiation mode (seeSection 18.12.1 on page 285), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL Device from IPSec routers with dynamic IP addresses (seeSection 18.18 on page 293 for a telecommuter configuration example).

Regardless of the ID type and content configuration, the ZyXEL Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (seeSection 18.12.1 on page 285), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (seeSection 18.13 on page 285). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 92 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL Device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 93 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL Device automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.

18.9.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyXEL Devices in this example can complete negotiation and establish a VPN tunnel.

Table 94 Matching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyXEL Devices in this example cannot complete their negotiation because ZyXEL Device B's **Local ID type** is **IP**, but ZyXEL Device A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 95 Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

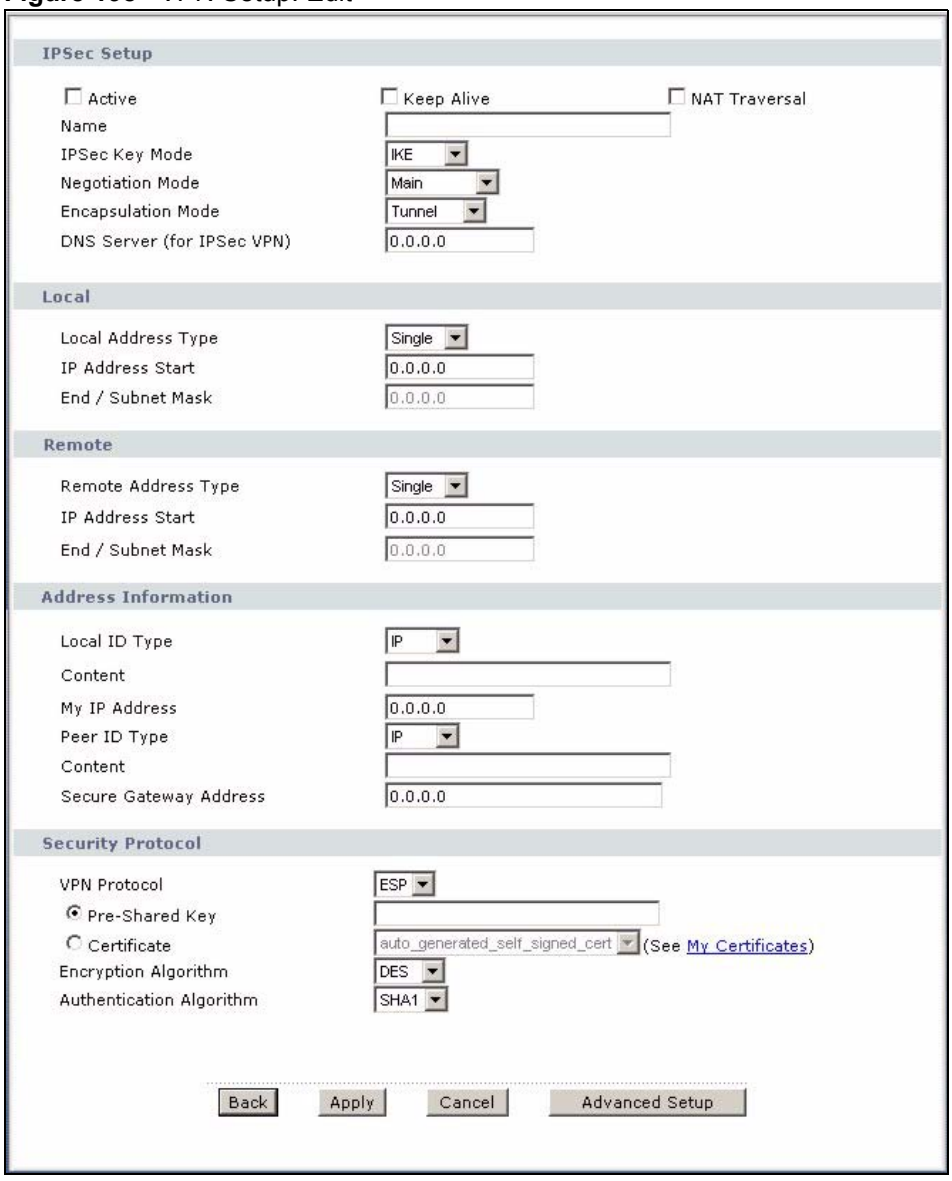
18.10 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (seeSection 18.12 on page 284for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

18.11 Editing VPN Policies

Click an **Edit** icon in the **VPN Setup** screen to edit VPN policies.

Figure 198 VPN Setup: Edit



The following table describes the fields in this screen.

Table 96 VPN Setup; Edit

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select either **Yes** or **No** from the drop-down list box. Select **Yes** to have the ZyXEL Device automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	This function is available if the **VPN Protocol** is **ESP**. Select this check box if you want to set up a VPN tunnel when there are NAT routers between the ZyXEL Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router.

Table 96 VPN Setup; Edit

LABEL	DESCRIPTION
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyXEL Device assigns this additional DNS server to the ZyXEL Device's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Specify the IP addresses of the devices behind the ZyXEL Device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyXEL Device.
Remote	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.

Table 96 VPN Setup; Edit

LABEL	DESCRIPTION
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Address Information	
Local ID Type	Select **IP** to identify this ZyXEL Device by its IP address. Select **DNS** to identify this ZyXEL Device by a domain name. Select **E-mail** to identify this ZyXEL Device by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyXEL Device automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. When there is a NAT router between the two IPSec routers. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyXEL Device in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
My IP Address	Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0**: The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See Chapter 8 on page 127 for details on dial backup and traffic redirect.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyXEL Device will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: When there is a NAT router between the two IPSec routers. When you want the ZyXEL Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.

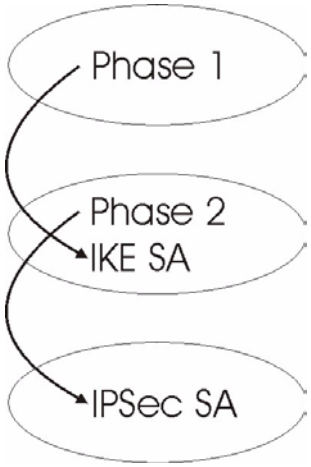
Table 96 VPN Setup; Edit

LABEL	DESCRIPTION
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Security Protocol	
VPN Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Pre-Shared Key	Click the button to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Click the button to use a certificate for authentication. Select the certificate you want to use from the list. You can create, import and configure certificates in the **Security > Certificates** screens, or click the **My Certificates** link.
My Certificates	Click this to go to the **Security > Certificates > My Certificates** screen. If you do not click **Apply** first, your VPN settings will not be saved.
Encryption Algorithm	Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click **Advanced Setup** to configure more detailed settings of your IKE key management.

18.12 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 199 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see Section 18.12.3 on page 285. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

18.12.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

18.12.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

18.12.3 Perfect Forward Secrecy (PFS)

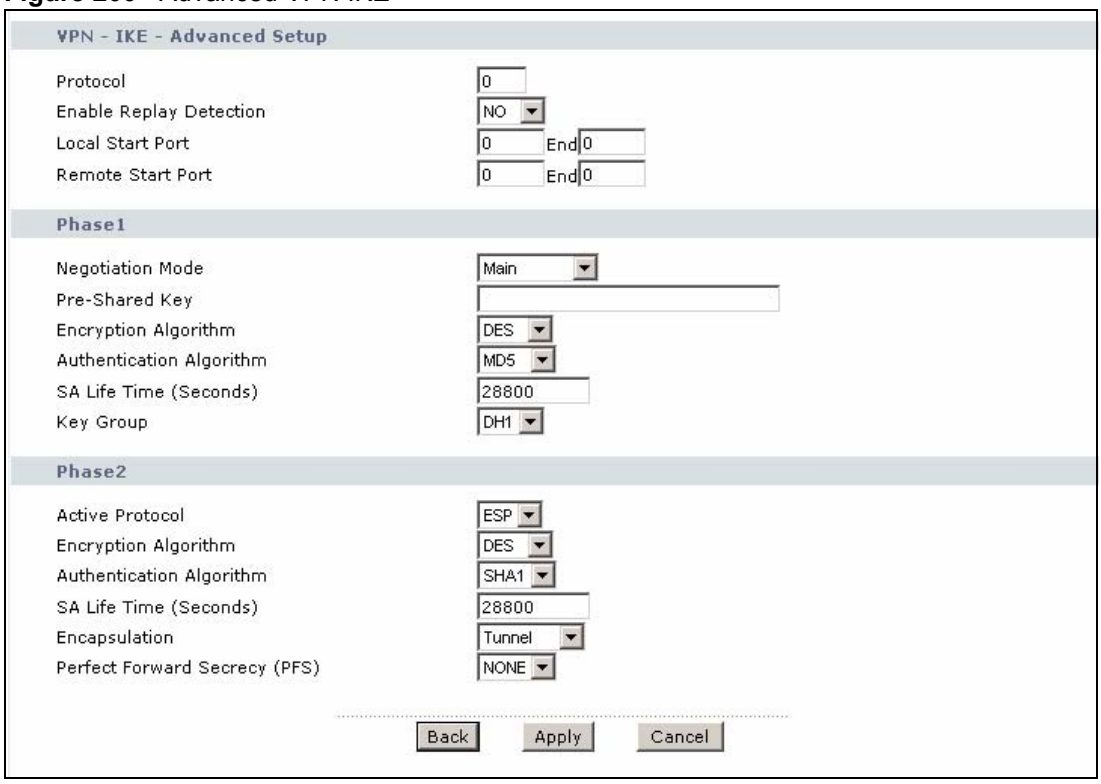
Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyXEL Device. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

18.13 Configuring Advanced IKE Settings

Click **Advanced Setup** in the **VPN Setup-Edit** screen to open this screen.

Figure 200 Advanced VPN IKE



The following table describes the fields in this screen.

Table 97 Advanced VPN IKE

LABEL	DESCRIPTION
VPN - IKE - Advanced Setup	
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Start Port** is left at 0, **End** will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Start Port** is left at 0, **End** will also remain at 0.
Phase 1	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Table 97 Advanced VPN IKE

LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Use the drop-down list box to choose from **ESP** or **AH**.
Encryption Algorithm	This field is available when you select **ESP** in the **Active Protocol** field. Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.

Table 97 Advanced VPN IKE

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH1** or **DH2** from the drop-down list box to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device and return to the **VPN-IKE** screen.
Cancel	Click **Cancel** to return to the **VPN-IKE** screen without saving your changes.

18.14 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

18.14.1 Security Parameter Index (SPI)

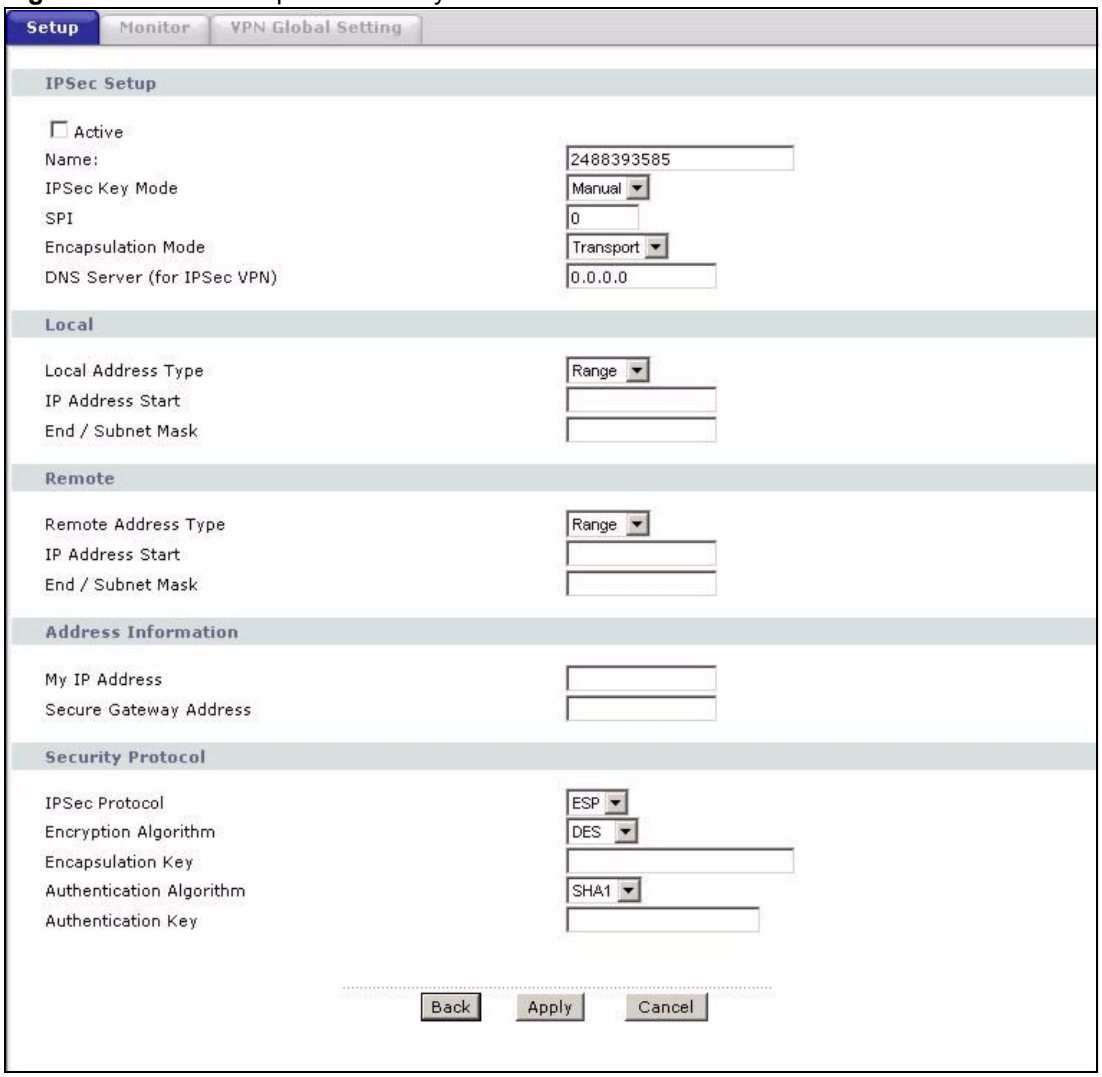
An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

18.15 Configuring Manual Key

You only configure VPN manual key when you select **Manual** in the **IPSec Key Mode** field on the **VPN Setup-Edit** screen. This is the **VPN Setup - Manual Key** screen as shown next.

Figure 201 VPN Setup: Manual Key



The following table describes the fields in this screen.

Table 98 VPN Setup: Manual Key

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.

Table 98 VPN Setup: Manual Key (continued)

LABEL	DESCRIPTION
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyXEL Device assigns this additional DNS server to the ZyXEL Device 's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyXEL Device.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to Single, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Address Information	

Table 98 VPN Setup: Manual Key (continued)

LABEL	DESCRIPTION
My IP Address	Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0**: The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See Chapter 8 on page 127 for details on dial backup and traffic redirect.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Security Protocol	
IPSec Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Encapsulation Key (only with ESP)	With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

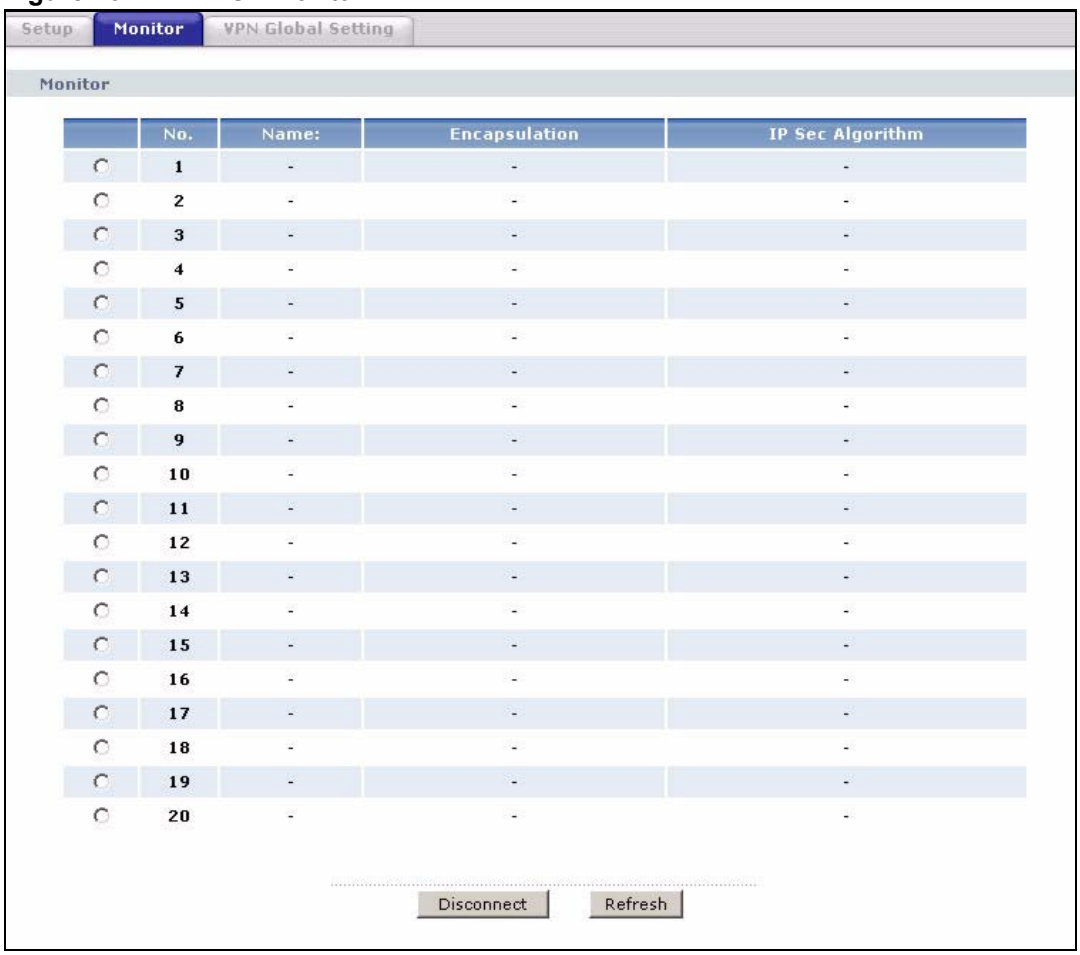
18.16 Viewing SA Monitor

Click **Security** > **VPN** > **Monitor** to open the screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See Section 18.6 on page 275on keep alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 202 VPN: SA Monitor



The following table describes the fields in this screen.

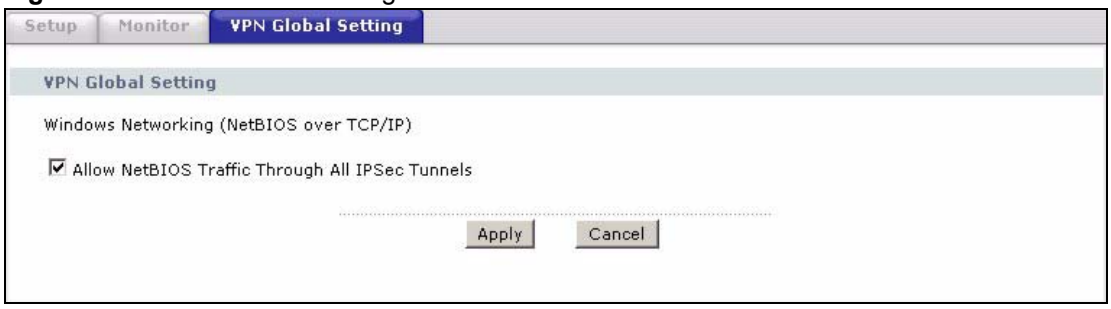
Table 99 VPN: SA Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocol, encryption algorithm, and authentication algorithm used in each VPN tunnel.
Disconnect	Select one of the security associations, and then click **Disconnect** to stop that security association.
Refresh	Click **Refresh** to display the current active VPN connection(s).

18.17 Configuring VPN Global Setting

To change your ZyXEL Device's global settings, click **VPN** > **VPN Global Setting**. The screen appears as shown.

Figure 203 VPN: Global Setting



The following table describes the fields in this screen.

Table 100 VPN: Global Setting

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through All IPSec Tunnels	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.18 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyXEL Device at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyXEL Device at headquarters has a static public IP address.

18.18.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyXEL Device at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 204 Telecommuters Sharing One VPN Rule Example

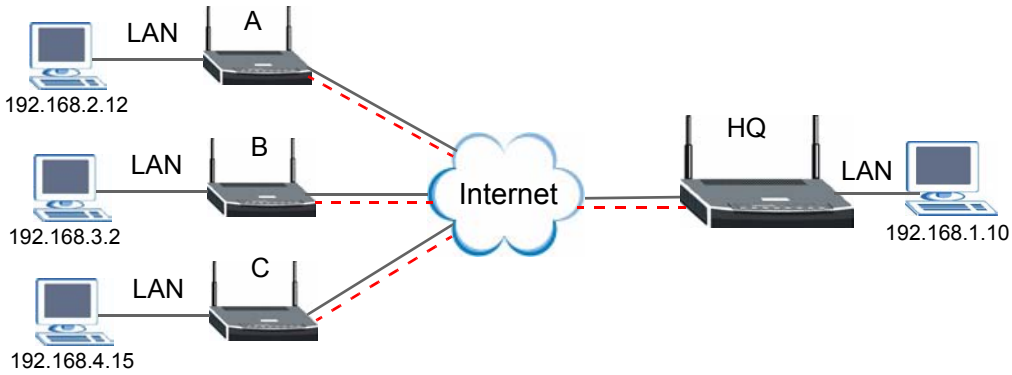


Table 101 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

18.18.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (**A**, **B** and **C** in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section 18.12.1 on page 285), the ZyXEL Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyXEL Device at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyXEL Device at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyXEL Device located at headquarters. The ZyXEL Device at headquarters (**HQ** in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyXEL Device at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 205 Telecommuters Using Unique VPN Rules Example

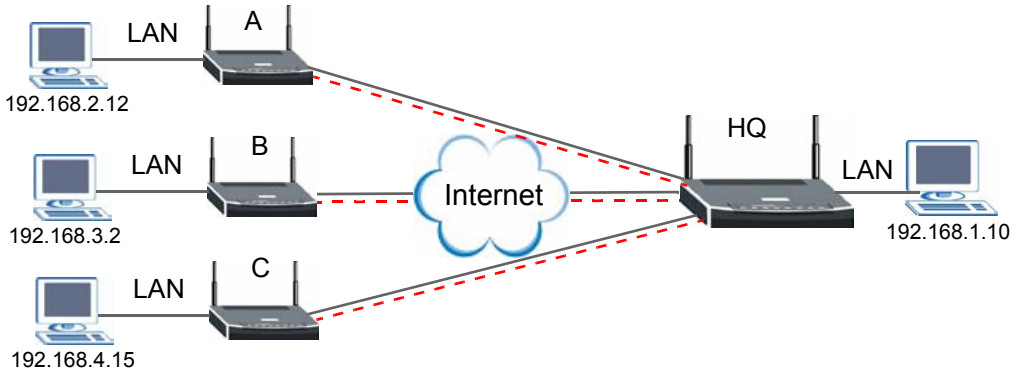


Table 102 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters ZyXEL Device Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters ZyXEL Device Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters ZyXEL Device Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

18.19 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote MGMT**) to allow access for that service.

19

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

19.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (Public-Key Infrastructure).

19.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

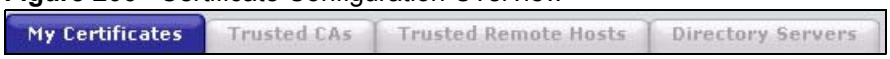
19.2 Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

19.3 Configuration Summary

This section summarizes how to manage certificates on the ZyXEL Device.

Figure 206 Certificate Configuration Overview



Use the **My Certificates** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.

Use the **Trusted CAs** screens to save CA certificates to the ZyXEL Device.

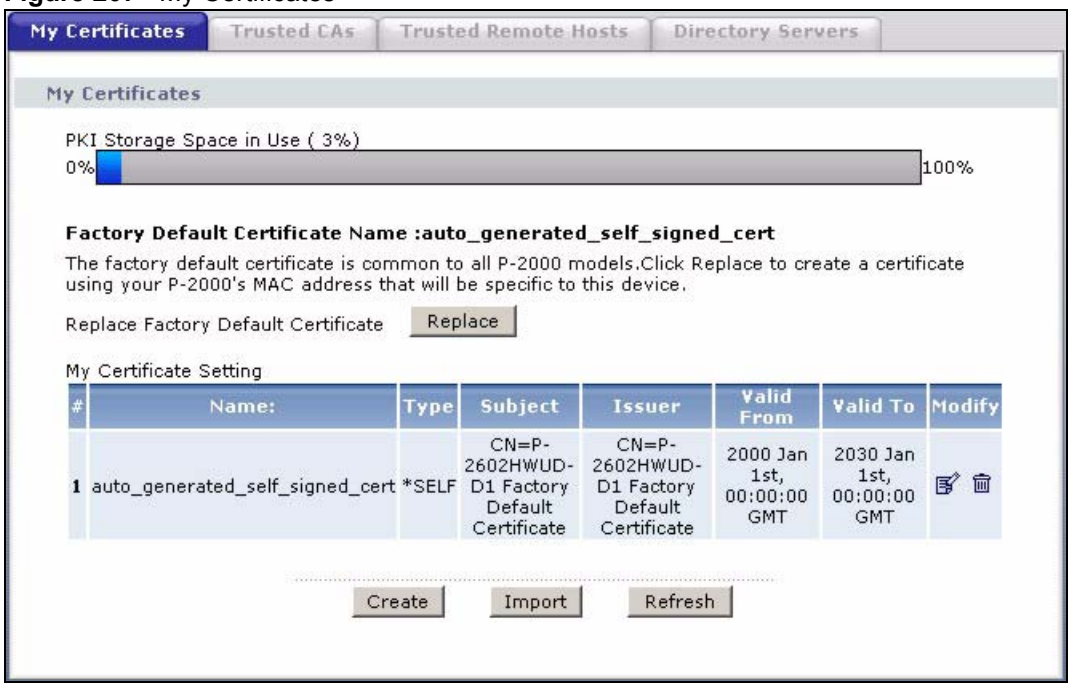
Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

19.4 My Certificates

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen. This is the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

Figure 207 My Certificates


My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
My Certificates
PKI Storage Space in Use (3%)
0%
100%
Factory Default Certificate Name :auto_generated_self_signed_cert
The factory default certificate is common to all P-2000 models.Click Replace to create a certificate using your P-2000's MAC address that will be specific to this device.
Replace Factory Default Certificate
Replace
My Certificate Setting
Name: Type Subject Issuer Valid From Valid To Modify
1 auto_generated_self_signed_cert *SELF CN=P-2602HWUD-D1 Factory Default Certificate CN=P-2602HWUD-D1 Factory Default Certificate 2000 Jan 1st, 00:00:00 GMT 2030 Jan 1st, 00:00:00 GMT
Create
Import
Refresh

The following table describes the labels in this screen.

Table 103 My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyXEL Device has the factory default certificate. The factory default certificate is common to all ZyXEL Devices that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyXEL Device's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.

Table 103 My Certificates (continued)

LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 2. Click the Edit icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action
Create	Click **Create** to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Refresh	Click **Refresh** to display the current validity status of the certificates.

19.5 My Certificate Import

Click **Security > Certificates > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.

You can only import a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

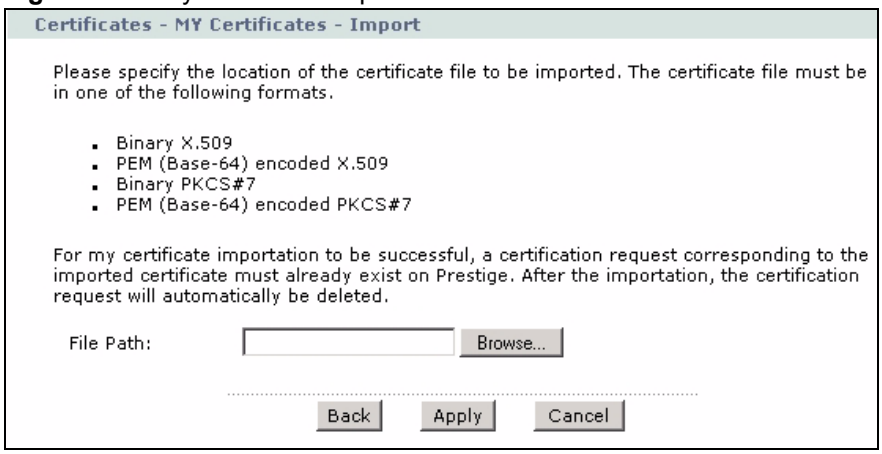
You must remove any spaces from the certificate's filename before you can import it.

19.5.1 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Figure 208 My Certificate Import


Certificates - MY Certificates - Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on Prestige. After the importation, the certification request will automatically be deleted.
File Path:
Browse...
Back
Apply
Cancel

The following table describes the labels in this screen.

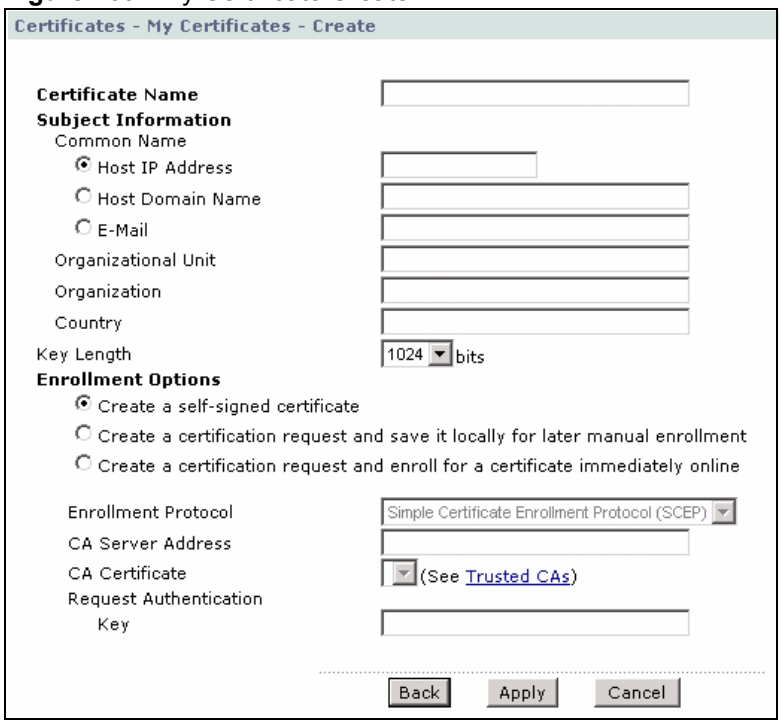
Table 104 My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to clear your settings.

19.6 My Certificate Create

Click **Security** > **Certificates** > **My Certificates** > **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 209 My Certificate Create



The following table describes the labels in this screen.

Table 105 My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.

Table 105 My Certificate Create (continued)

LABEL	DESCRIPTION
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyXEL Device generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 19.7 on page 304) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

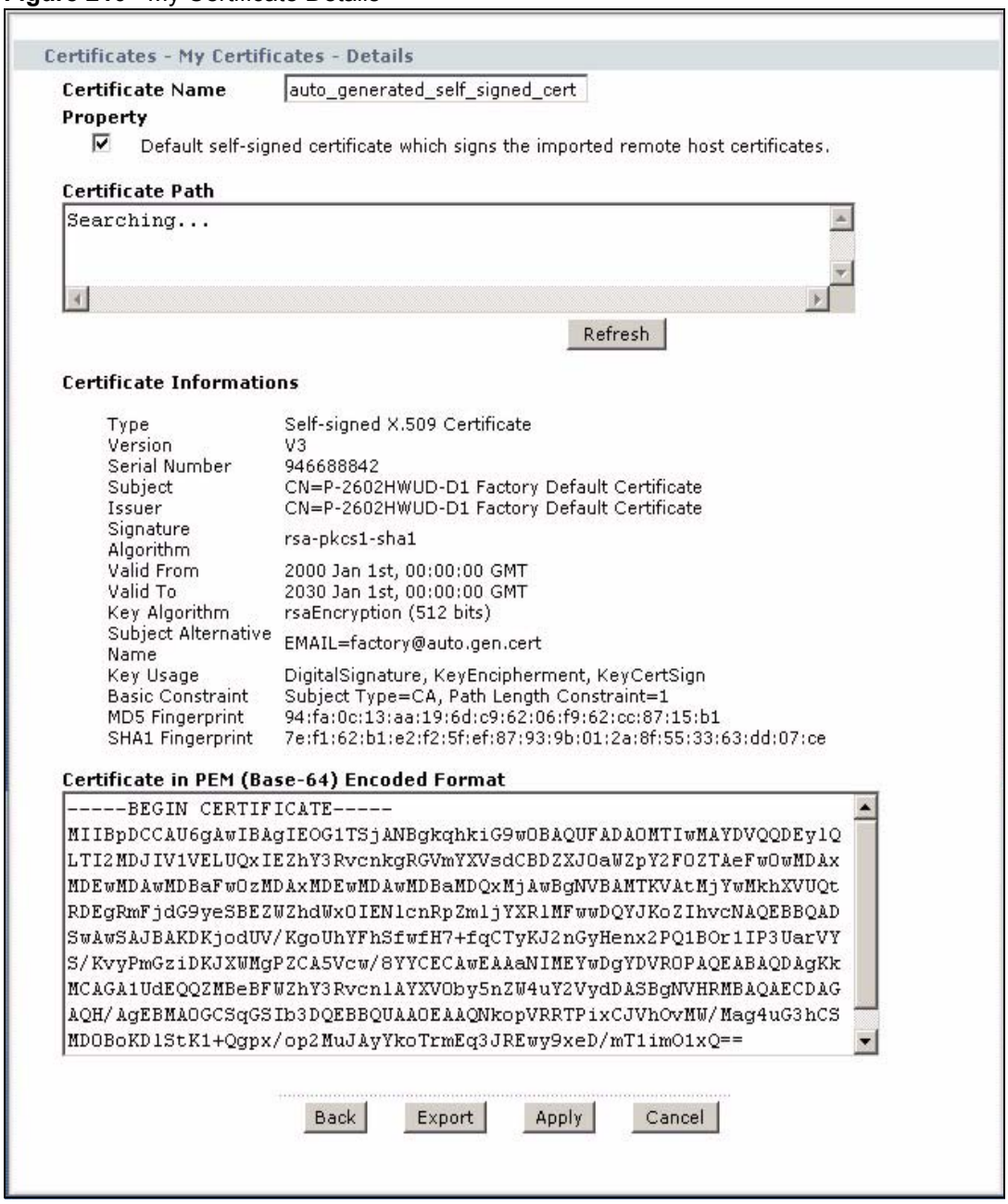
After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

19.7 My Certificate Details

Click **Security** > **Certificates** > **My Certificates** to open the **My Certificates** screen (see Figure 207 on page 299). Click the edit icon to open the **My Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device.

Figure 210 My Certificate Details



The following table describes the labels in this screen.

Table 106 My Certificate Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).

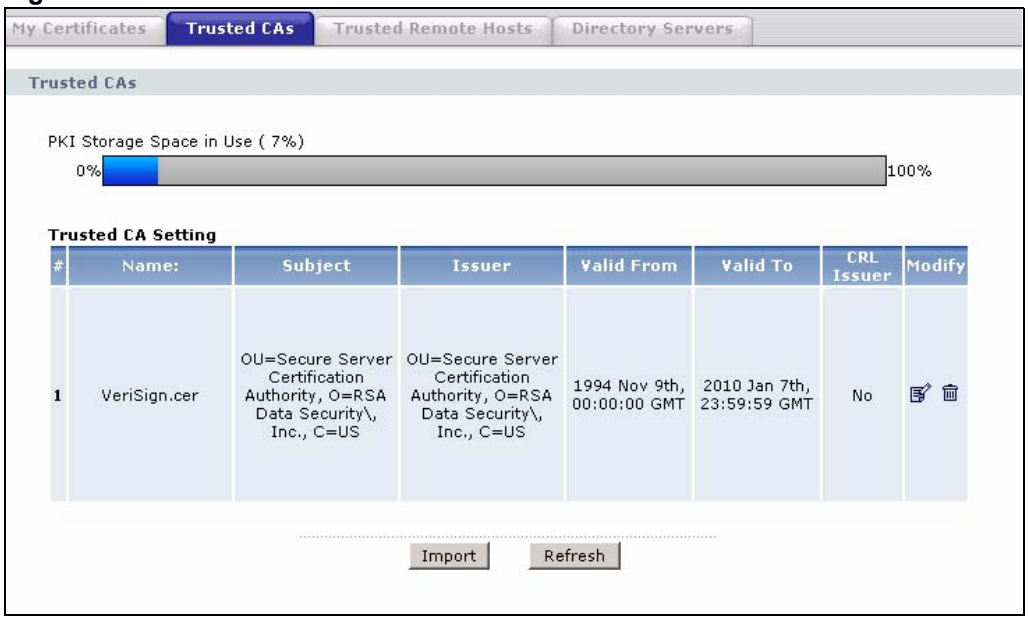
Table 106 My Certificate Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

19.8 Trusted CAs

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 211 Trusted CAs



The following table describes the labels in this screen.

Table 107 Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from blue to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".

Table 107 Trusted CAs (continued)

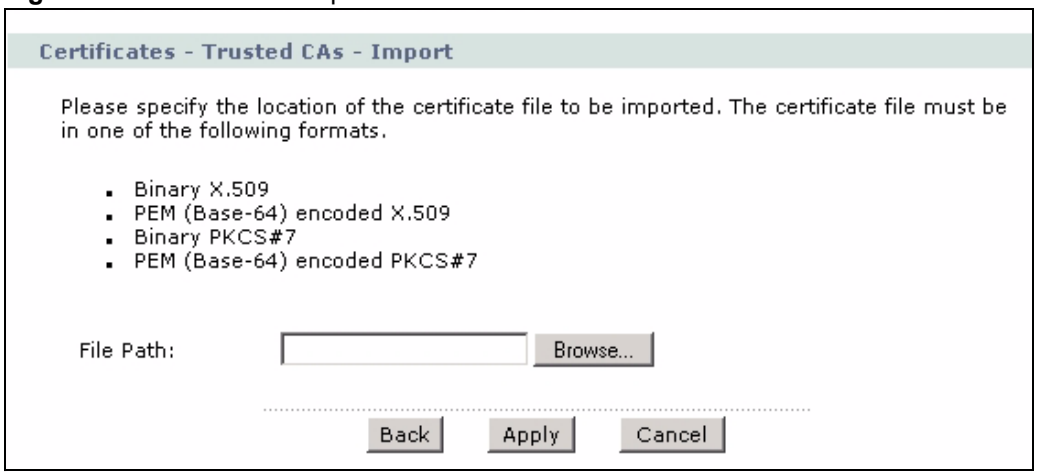
LABEL	DESCRIPTION
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

19.9 Trusted CA Import

Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device.

You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 212 Trusted CA Import


Certificates - Trusted CAs - Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path:
Browse...
Back
Apply
Cancel

The following table describes the labels in this screen.

Table 108 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

19.10 Trusted CA Details

Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 213 Trusted CA Details

The following table describes the labels in this screen.

Table 109 Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Issues certificate revocation lists (CRLs)	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).

Table 109 Trusted CA Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

19.11 Trusted Remote Hosts

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyXEL Device automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 214 Trusted Remote Hosts

My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
Trusted Remote Hosts
PKI Storage Space in Use (7%)
0%
100%
Trusted Remote Host Certificates
Issuer (My Default Self-signed Certificate): CN=P-2602HWL-D1A 001349000001
Name: Subject Valid From Valid To Modify
1 VeriSign.cer OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US 1994 Nov 9th, 00:00:00 GMT 2010 Jan 7th, 23:59:59 GMT
Import
Refresh

The following table describes the labels in this screen.

Table 110 Trusted Remote Hosts

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

19.12 Verifying a Trusted Remote Host's Certificate

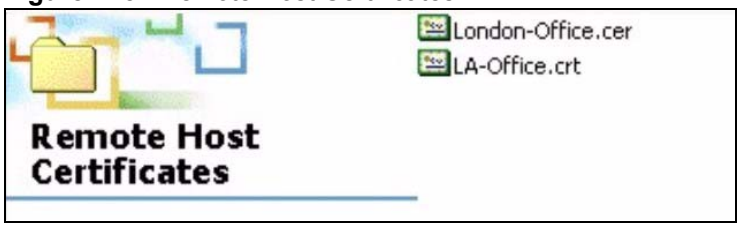
Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

19.12.1 Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

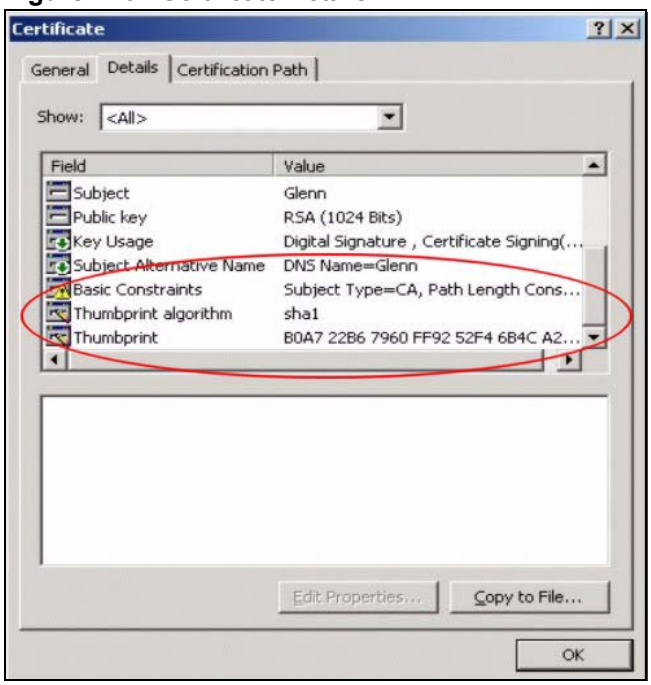
1. Browse to where you have the remote host's certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 215 Remote Host Certificates



3. Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 216 Certificate Details



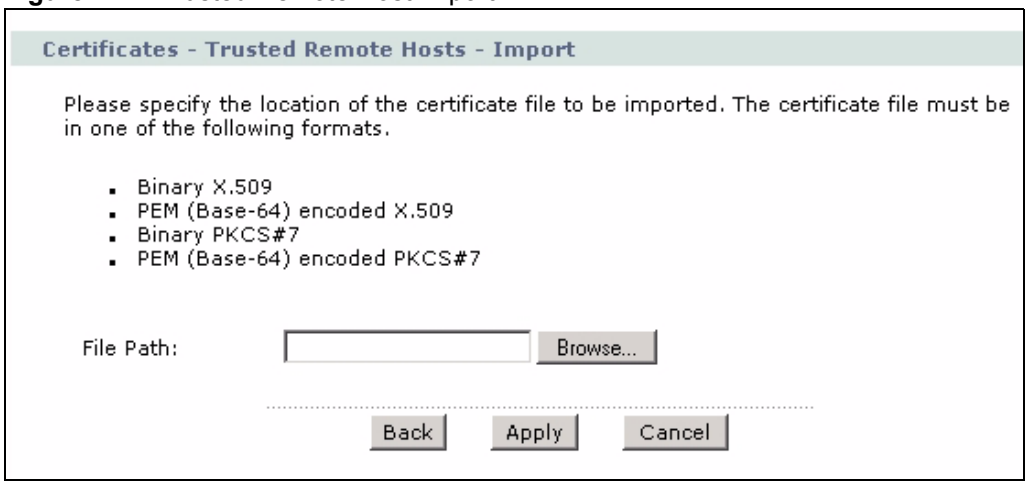
Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

19.13 Trusted Remote Hosts Import

Click **Security** > **Certificates** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the ZyXEL Device.

The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

Figure 217 Trusted Remote Host Import


Certificates - Trusted Remote Hosts - Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path:
Browse...
Back
Apply
Cancel

The following table describes the labels in this screen.

Table 111 Trusted Remote Host Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen.

19.14 Trusted Remote Host Certificate Details

Click **Security** > **Certificates** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. Use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

Figure 218 Trusted Remote Host Details

The following table describes the labels in this screen.

Table 112 Trusted Remote Host Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyXEL Device uses to sign remote host certificates.

Table 112 Trusted Remote Host Details (continued)

LABEL	DESCRIPTION
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyXEL Device is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyXEL Device used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 19.12 on page 314 for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 19.12 on page 314 for how to verify a remote host's certificate.

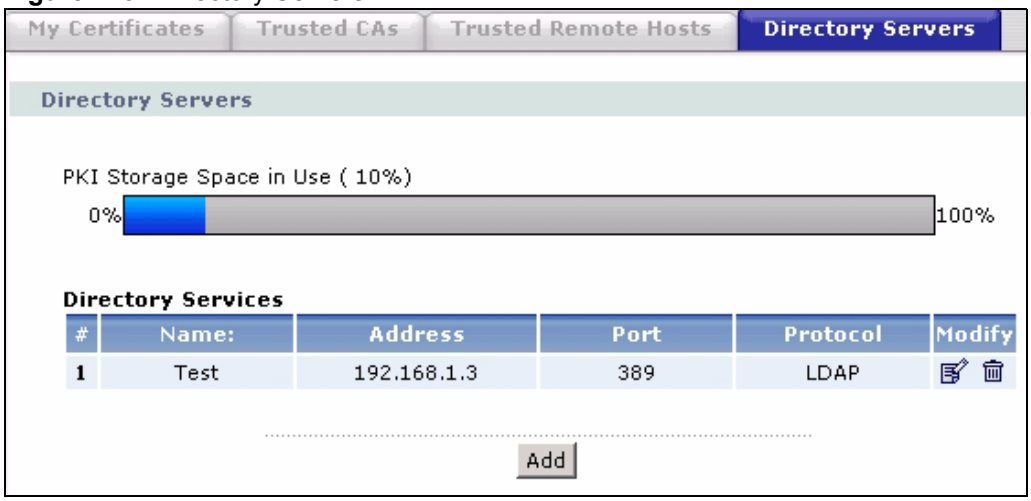
Table 112 Trusted Remote Host Details (continued)

LABEL	DESCRIPTION
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name of the certificate.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen.

19.15 Directory Servers

Click **Security** > **Certificates** > **Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyXEL Device. If you decide to have the ZyXEL Device check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyXEL Device first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyXEL Device checks the servers listed here.

Figure 219 Directory Servers



The following table describes the labels in this screen.

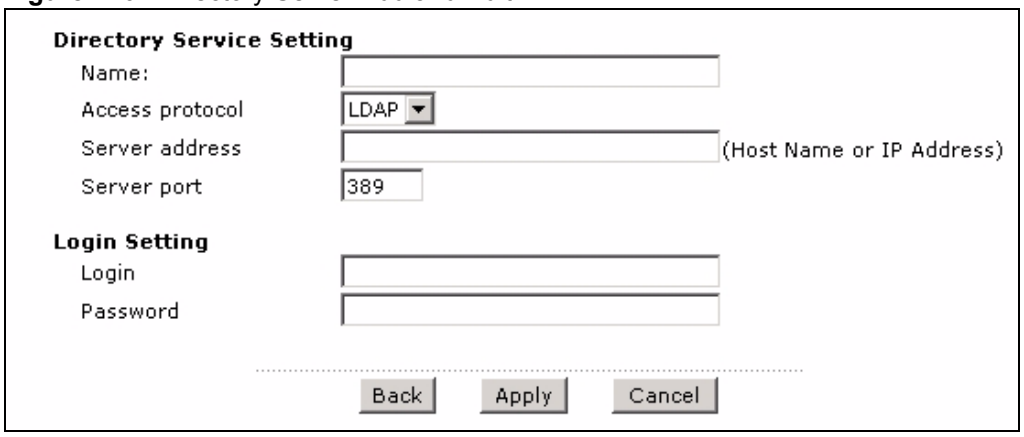
Table 113 Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the Edit icon to open a screen where you can change the information about the directory server. Click the Remove icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click **Add** to open a screen where you can configure information about a directory server so that the ZyXEL Device can access it.

19.16 Directory Server Add and Edit

Click **Security** > **Certificates** > **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyXEL Device can access.

Figure 220 Directory Server Add and Edit



The following table describes the labels in this screen.

Table 114 Directory Server Add and Edit

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.

Table 114 Directory Server Add and Edit

LABEL	DESCRIPTION
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.[A]
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the **Access Protocol** field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyXEL Device may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Back	Click **Back** to return to the **Directory Servers** screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to quit configuring this screen.

A. At the time of writing, LDAP is the only choice of directory server access protocol.

20

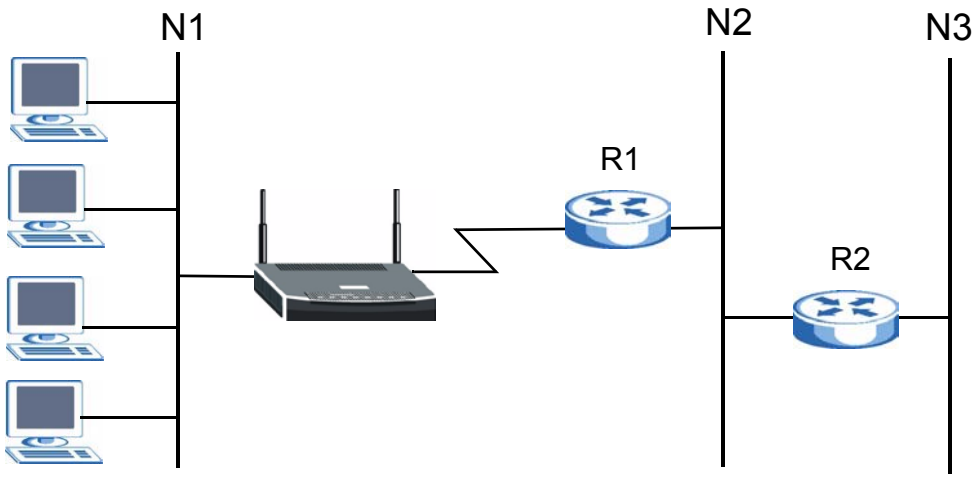
Static Route

This chapter shows you how to configure static routes for your ZyXEL Device.

20.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

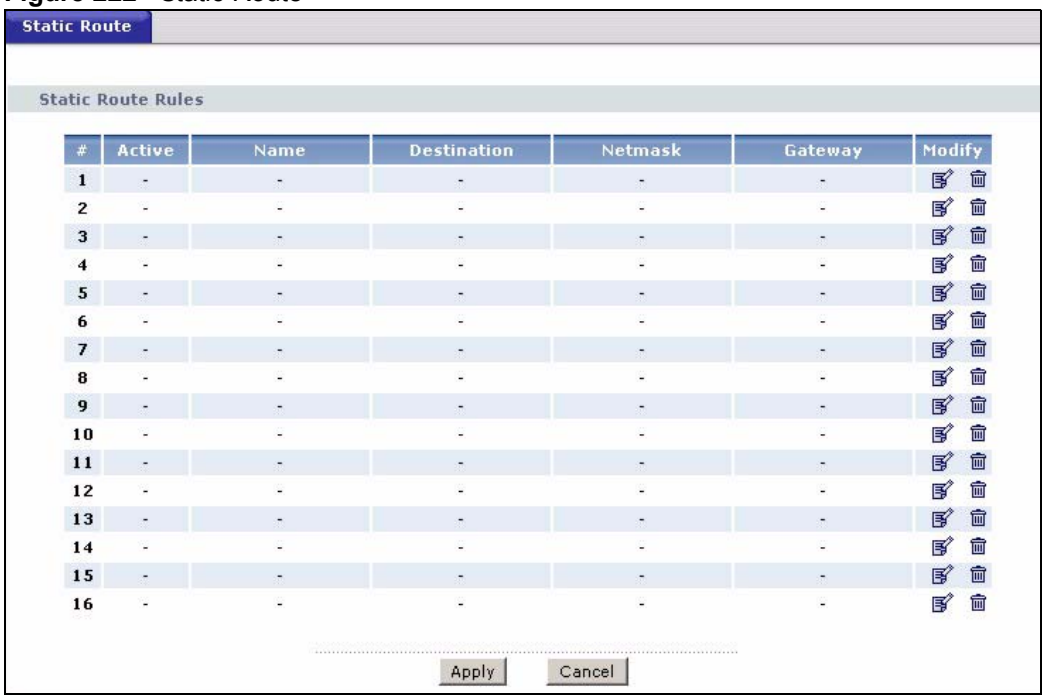
Figure 221 Example of Static Routing Topology



20.2 Configuring Static Route

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 222 Static Route


Static Route
Static Route Rules
Active Name Destination Netmask Gateway Modify
1 - - - - -
2 - - - - -
3 - - - - -
4 - - - - -
5 - - - - -
6 - - - - -
7 - - - - -
8 - - - - -
9 - - - - -
10 - - - - -
11 - - - - -
12 - - - - -
13 - - - - -
14 - - - - -
15 - - - - -
16 - - - - -
Apply
Cancel

The following table describes the labels in this screen.

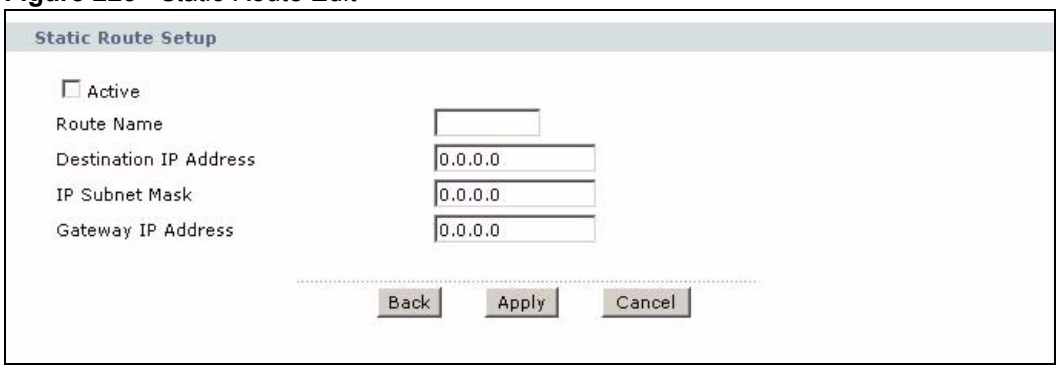
Table 115 Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the Remove icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Apply	Click this to apply your changes to the ZyXEL Device.
Cancel	Click this to return to the previously saved configuration.

20.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 223 Static Route Edit



The following table describes the labels in this screen.

Table 116 Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21

Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the ZyXEL Device's bandwidth management logs.

21.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on application. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The ZyXEL Device applies bandwidth management to traffic that it forwards out through an interface. The ZyXEL Device does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.

21.2 Application-based Bandwidth Management

You can create bandwidth classes based on individual applications (like Web, FTP and E-mail, for example).

21.3 Auto Classifier

Automatic Traffic Classifier (ATC) is a bandwidth management tool that prioritizes data packets sent across the network. ATC assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

ATC assigns priority based on packet size, since time-sensitive applications such as Internet telephony (Voice over IP or VoIP) tend to have smaller packet sizes than non-time sensitive applications such as FTP (File Transfer Protocol). The following table shows some common applications, their time sensitivity, and their typical data packet sizes. Note that the figures given are merely examples - sizes may differ according to application and circumstances.

Table 117 Typical Packet Sizes

APPLICATION	TIME SENSITIVITY	TYPICAL PACKET SIZE (BYTES)
Voice over IP (SIP)	High	< 250
Online Gaming	High	60 ~ 90
Web browsing (http)	Medium	300 ~ 600
FTP	Low	1500

When ATC is activated, the device sends traffic with smaller packets before traffic with larger packets if the network is congested.

ATC assigns priority to packets as shown in the following table.

Table 118 Automatic Traffic Classifier Priorities

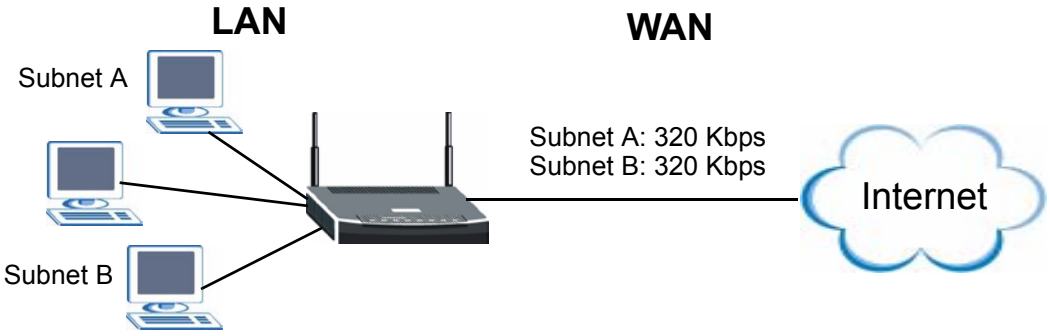
PACKET SIZE (BYTES)	ATC PRIORITY
1 ~ 250	ATC_High
250 ~ 1100	ATC_Medium
1100 +	ATC_Low

21.4 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

Figure 224 Subnet-based Bandwidth Management Example



21.5 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 119 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP (SIP)	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps

21.5.1 Bandwidth Management Priorities

Traffic with a higher priority gets through faster while traffic with a lower priority is dropped if the network is congested. The following table describes the priorities that you can apply to traffic that the ZyXEL Device forwards out through an interface.

Table 120 Bandwidth Management Priorities

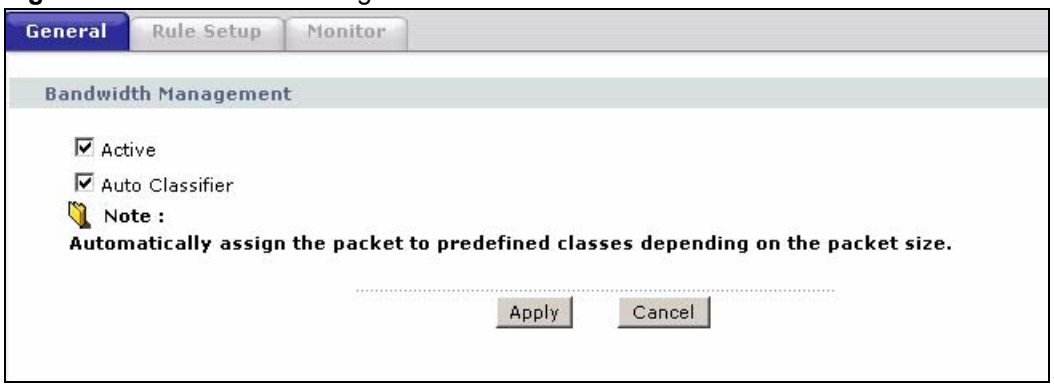
PRIORITY	DESCRIPTION
High	Typically used for voice traffic or video that is especially sensitive to jitter (variations in delay).
Mid	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.

21.6 Configuring Bandwidth Management (General)

Click **Advanced > Bandwidth MGMT** to open the screen as shown next.

Use this screen to enable or disable bandwidth management, and to enable or disable automatic traffic classification.

Figure 225 Bandwidth Management: General



The following table describes the labels in this screen.

Table 121 Bandwidth Management: General

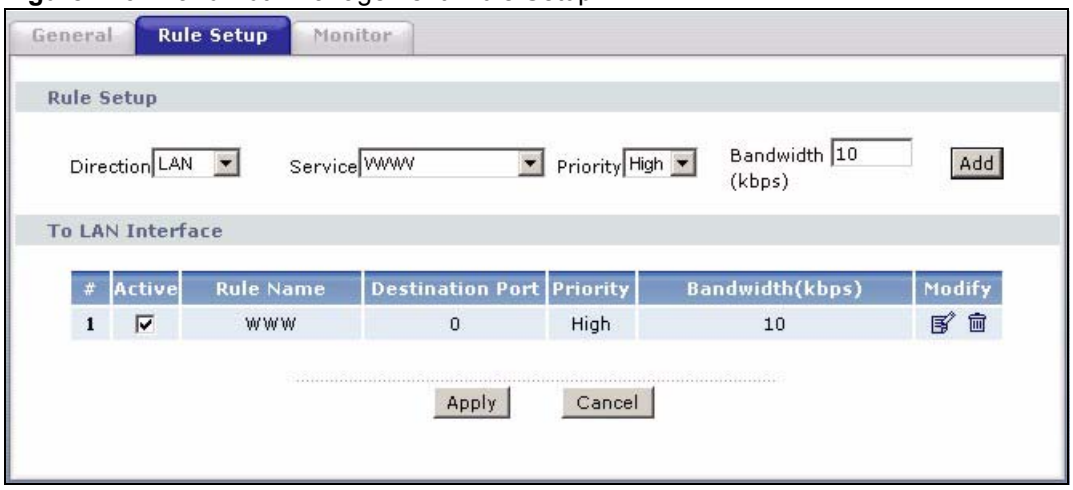
LABEL	DESCRIPTION
Active	Select the check box to enable bandwidth management.
Auto Classifier	Select the check box to enable Automatic Traffic Classifier (ATC). ATC assigns each packet to a bandwidth management class based on its size, since time-sensitive applications such as VoIP tend to have smaller packet sizes than non-time sensitive applications such as FTP. When ATC is enabled, traffic with a smaller packet size is assigned a higher priority than traffic with a larger packet size.
Apply	Click **Apply** to save your settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.7 Bandwidth Management Rule Setup

You must use the **Bandwidth Management General** screen to enable bandwidth management before you can configure rules.

Click **Advanced > Bandwidth MGMT > Rule Setup** to open the following screen.

Figure 226 Bandwidth Management: Rule Setup



The following table describes the labels in this screen.

Table 122 Bandwidth Management: Rule Setup

LABEL	DESCRIPTION
Direction	Select **LAN** to apply bandwidth management to traffic that the ZyXEL Device forwards to the LAN. Select **WAN** to apply bandwidth management to traffic that the ZyXEL Device forwards to the WAN. Select **WLAN** to apply bandwidth management to traffic that the ZyXEL Device forwards to the WLAN.
Service	Select a service for your rule or you can select **User define** to go to the screen where you can define your own.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.

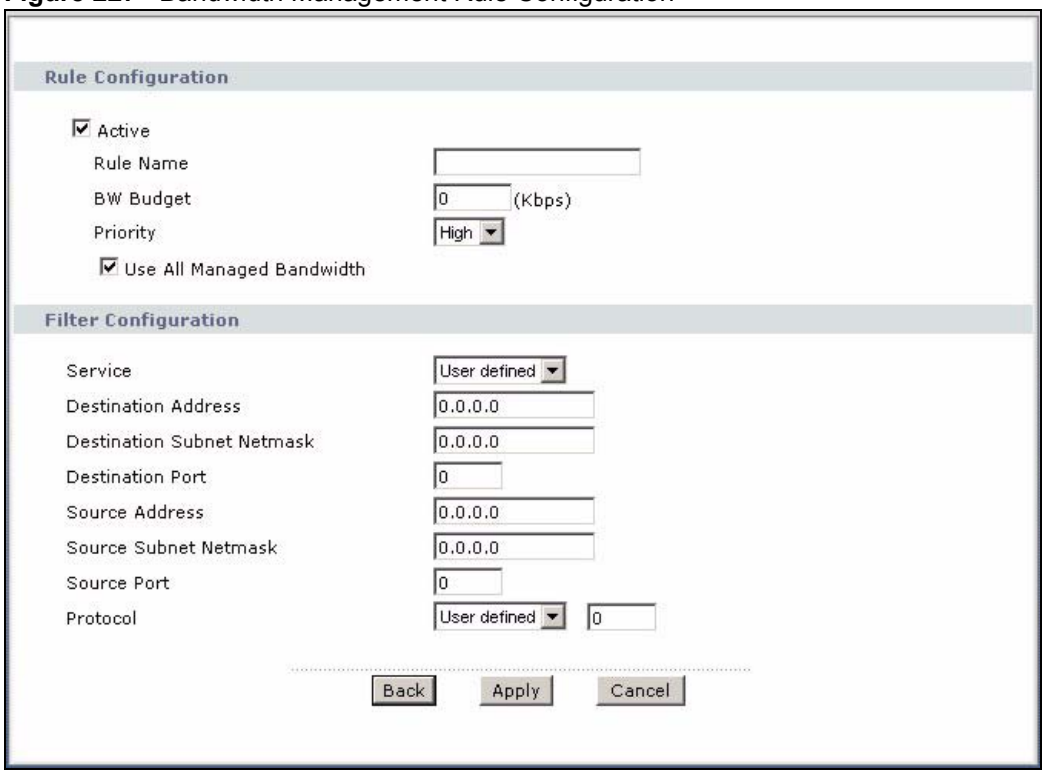
Table 122 Bandwidth Management: Rule Setup (continued)

LABEL	DESCRIPTION
Bandwidth (kbps)	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule. If you want to leave some bandwidth for traffic that does not match a bandwidth filter, make sure that the interface's root class has more bandwidth than the sum of the bandwidths of the interface's bandwidth management rules.
Add	Click this button to save your rule. It displays in the following table.
#	This is the number of an individual bandwidth management rule.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Rule Name	This is the name of the rule.
Destination Port	This is the port number of the destination. 0 means any destination port.
Priority	This is the priority of this rule.
Bandwidth (kbps)	This is the maximum bandwidth allowed for the rule in kbps.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.7.1 Rule Configuration

Click the **Edit** icon or **User defined** in the **Service** field to configure a bandwidth management rule. Use bandwidth rules to allocate specific amounts of bandwidth capacity (bandwidth budgets) to specific applications and/or subnets.

Figure 227 Bandwidth Management Rule Configuration



See Appendix E on page 499 for a list of commonly-used services. The following table describes the labels in this screen.

Table 123 Bandwidth Management Rule Configuration

LABEL	DESCRIPTION
Rule Configuration	
Active	Select the check box to enable the rule.
Rule Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.
Use All Managed Bandwidth	Select this option to allow a rule to borrow unused bandwidth on the interface. Bandwidth borrowing is governed by the priority of the rules. That is, a rule with the highest priority is the first to borrow bandwidth. Do not select this if you want to leave bandwidth available for other traffic types or if you want to restrict the amount of bandwidth that can be used for the traffic that matches this rule.
Filter Configuration	

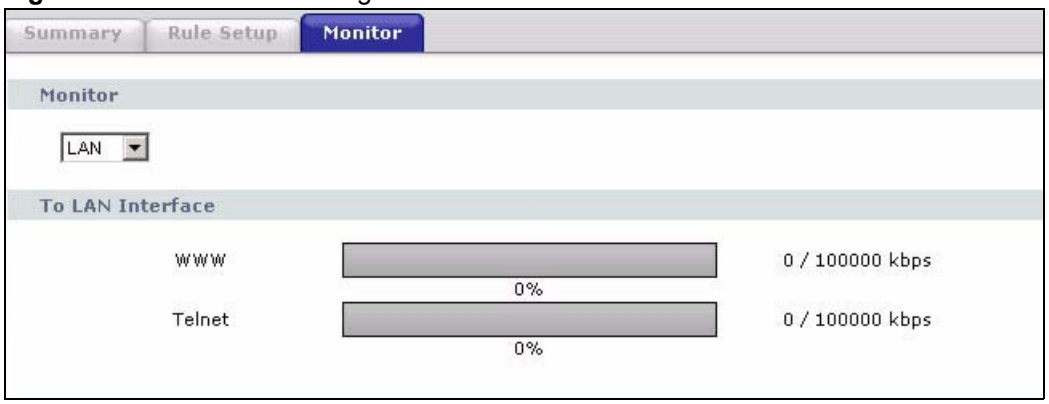
Table 123 Bandwidth Management Rule Configuration (continued)

LABEL	DESCRIPTION
Service	This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter). SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select **SIP** from the drop-down list box to configure this bandwidth filter for traffic that uses SIP. File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select **FTP** from the drop-down list box to configure this bandwidth filter for FTP traffic. H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select **H.323** from the drop-down list box to configure this bandwidth filter for traffic that uses H.323. Select **User defined** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **User defined**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address).
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination Address**. Refer to the appendix for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See Appendix E on page 499 for some common services and port numbers. A blank destination IP address means any destination IP address.
Source Address	Enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a **Source Address**. Refer to the appendix for more information on IP subnetting. A blank source port means any source port number.
Source Port	Enter the port number of the source. See Appendix E on page 499 for some common services and port numbers.
Protocol	Select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number. 0 means any protocol number.
Back	Click **Back** to go to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.8 Bandwidth Monitor

To view the ZyXEL Device's bandwidth usage, click **Advanced > Bandwidth MGMT > Monitor**. The screen appears as shown. Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth rules. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 228 Bandwidth Management: Monitor



22

Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

22.1 Dynamic DNS Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

22.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

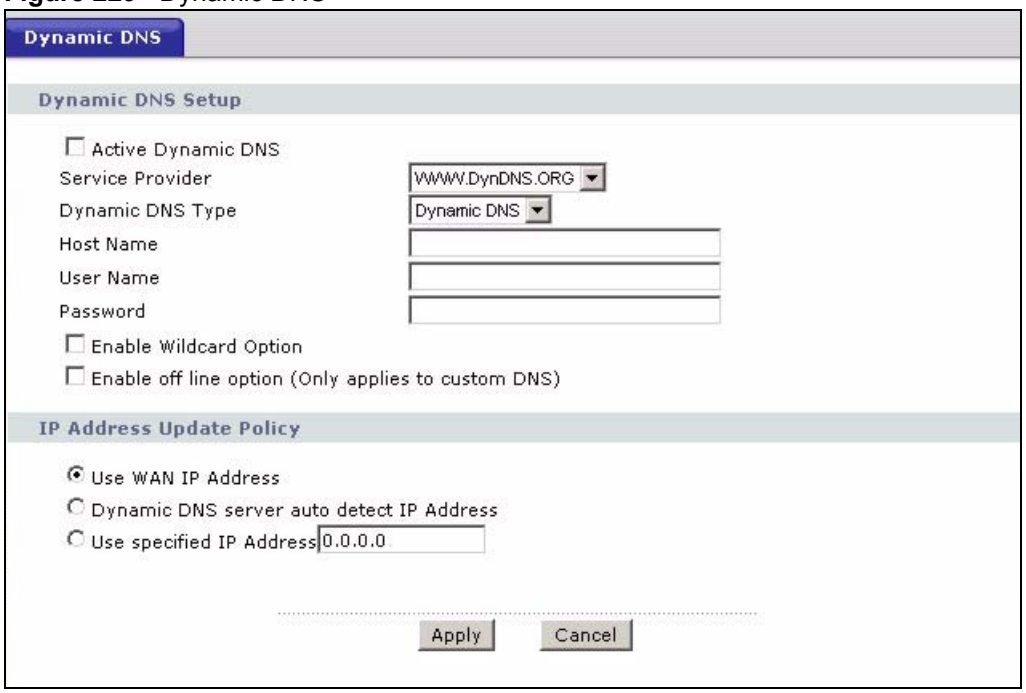
See Section 22.2 on page 333 for configuration instruction.

22.2 Configuring Dynamic DNS

To change your ZyXEL Device's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

See Section 22.1 on page 333 for more information.

Figure 229 Dynamic DNS



The following table describes the fields in this screen.

Table 124 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.

Table 124 Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23

Remote Management Configuration

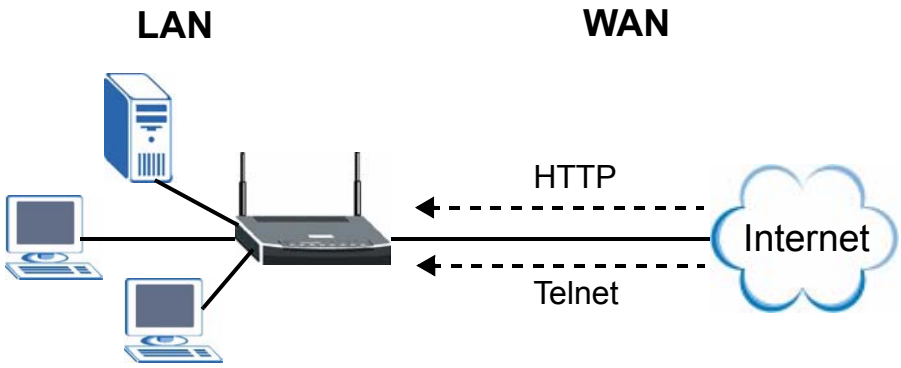
This chapter provides information on configuring remote management.

23.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

The following figure shows remote management of the ZyXEL Device coming in from the WAN.

Figure 230 Remote Management From the WAN



When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

When you choose **WAN** only or **LAN & WAN**, you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

23.1.1 Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

23.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

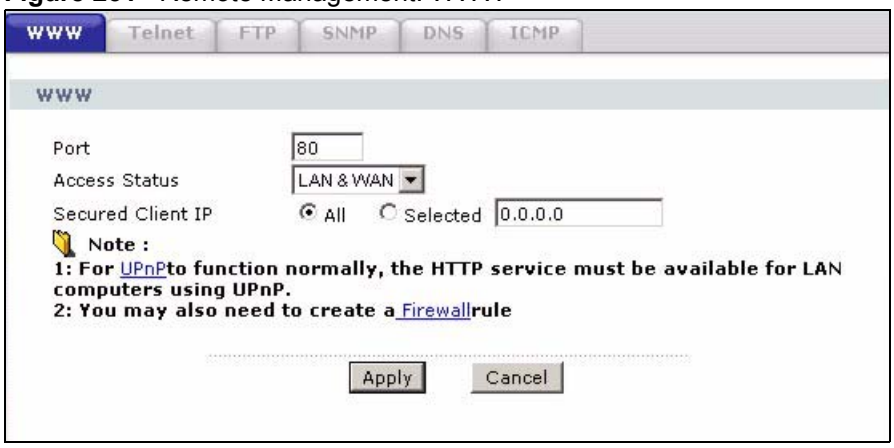
23.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

23.2 WWW

To change your ZyXEL Device's World Wide Web settings, click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 231 Remote Management: WWW



The following table describes the labels in this screen.

Table 125 Remote Management: WWW

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

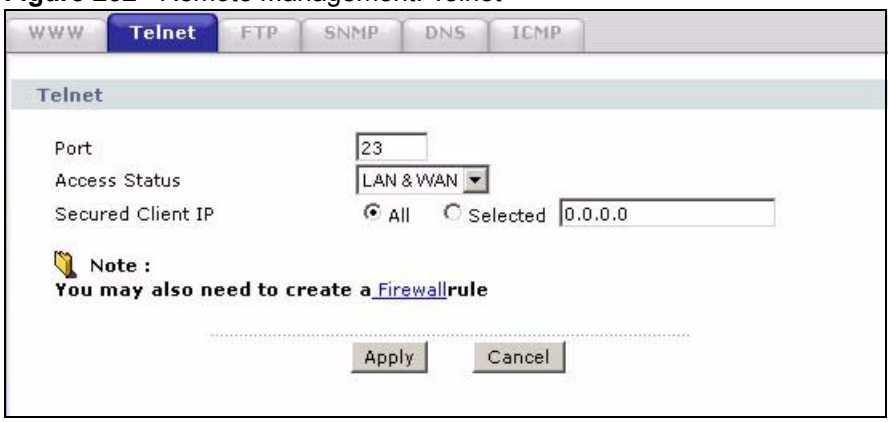
23.3 Telnet

You can use Telnet to access the ZyXEL Device’s command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

23.4 Configuring Telnet

Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 232 Remote Management: Telnet



The following table describes the labels in this screen.

Table 126 Remote Management: Telnet

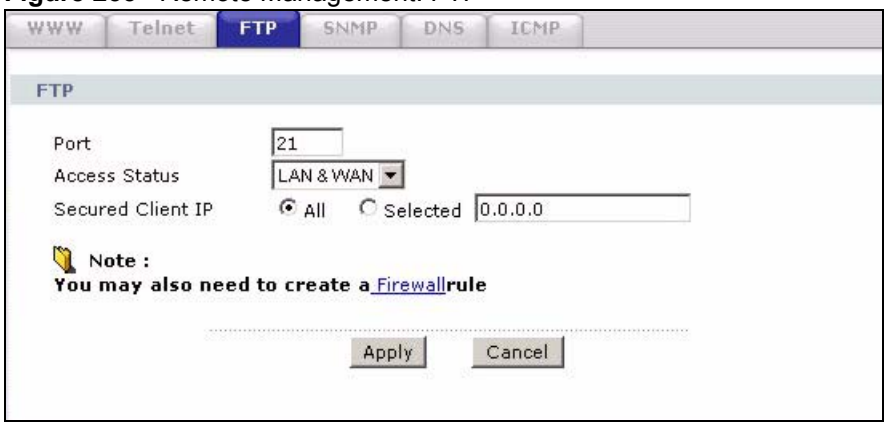
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.5 Configuring FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyXEL Device’s firmware and configuration files, please see the User’s Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device’s FTP settings, click **Advanced > Remote MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

Figure 233 Remote Management: FTP



The following table describes the labels in this screen.

Table 127 Remote Management: FTP

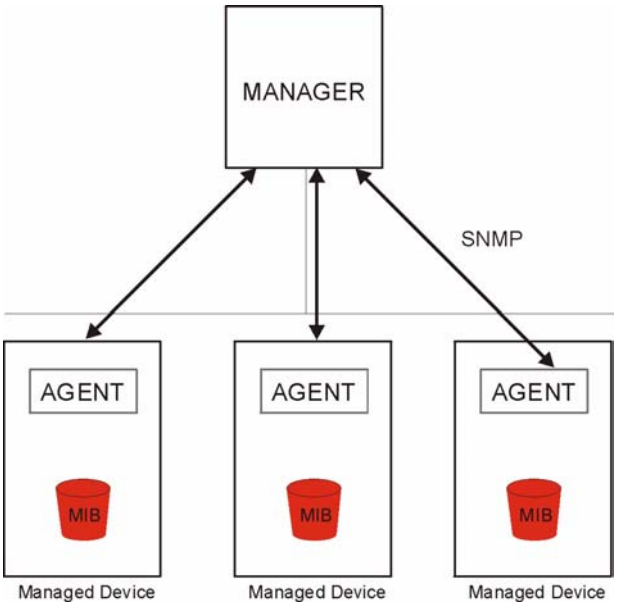
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

SNMP is only available if TCP/IP is configured.

Figure 234 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

23.6.1 Supported MIBs

The ZyXEL Device supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

23.6.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

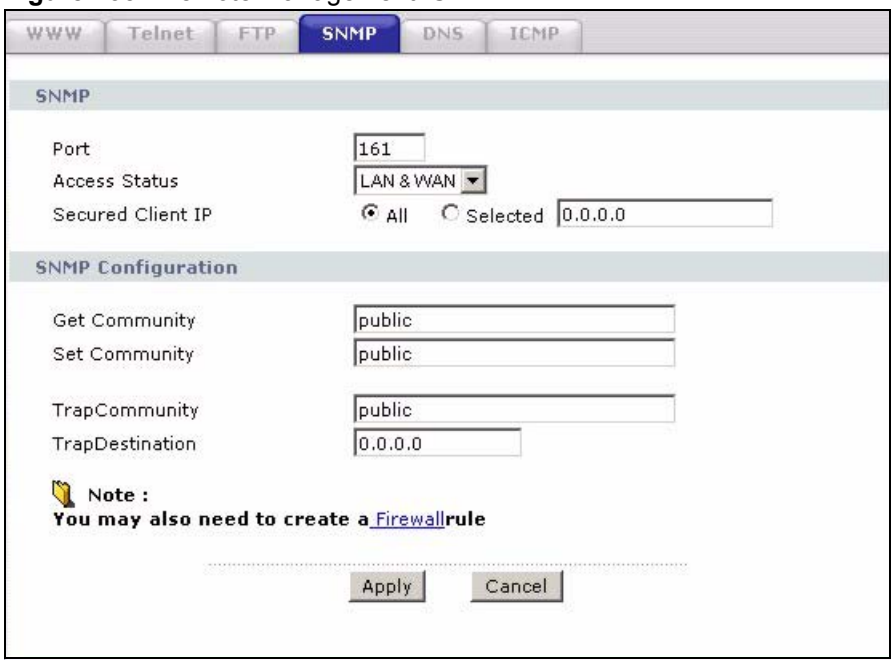
Table 128 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

23.6.3 Configuring SNMP

To change your ZyXEL Device's SNMP settings, click **Advanced > Remote MGMT** > **SNMP**. The screen appears as shown.

Figure 235 Remote Management: SNMP



The following table describes the labels in this screen.

Table 129 Remote Management: SNMP

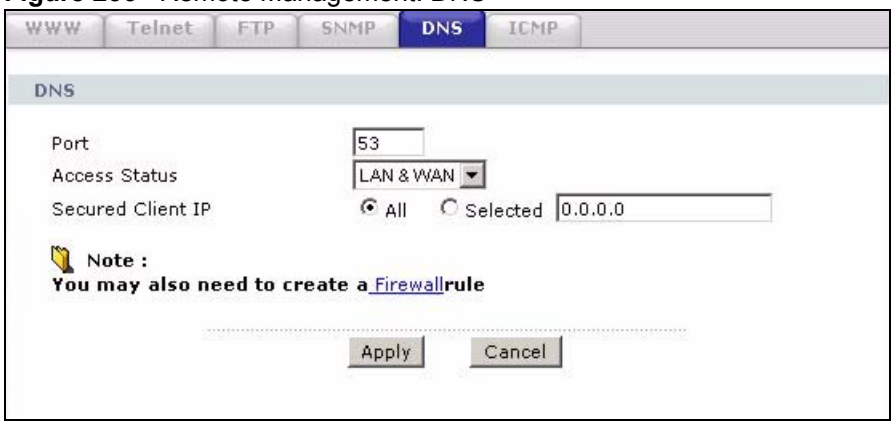
LABEL	DESCRIPTION
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 7 on page 89 for background information.

Click **Advanced > Remote MGMT** > **DNS** to change your ZyXEL Device’s DNS settings. Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device’s DNS settings. This feature is not available when the ZyXEL Device is set to bridge mode.

Figure 236 Remote Management: DNS



The following table describes the labels in this screen.

Table 130 Remote Management: DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured client is a “trusted” computer that is allowed to send DNS queries to the ZyXEL Device. Select **All** to allow any computer to send DNS queries to the ZyXEL Device. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

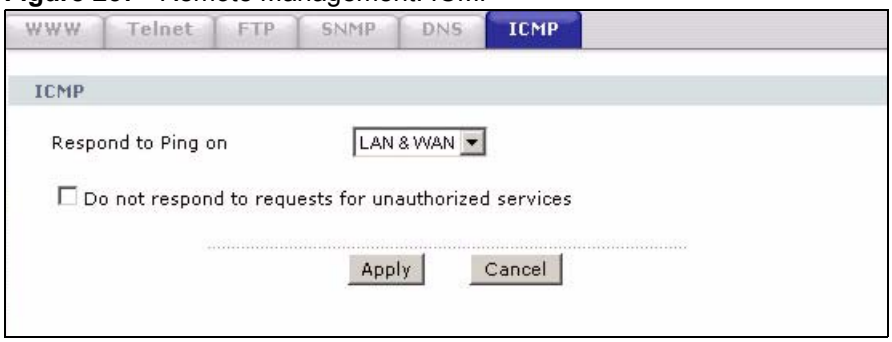
23.8 Configuring ICMP

To change your ZyXEL Device’s security settings, click **Advanced > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

Figure 237 Remote Management: ICMP



The following table describes the labels in this screen.

Table 131 Remote Management: ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. If this option is not selected, the ZyXEL Device will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyXEL Device's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyXEL Device reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

24.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See Section 24.2.1 on page 348 for configuration instructions.

24.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

24.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

24.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

24.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

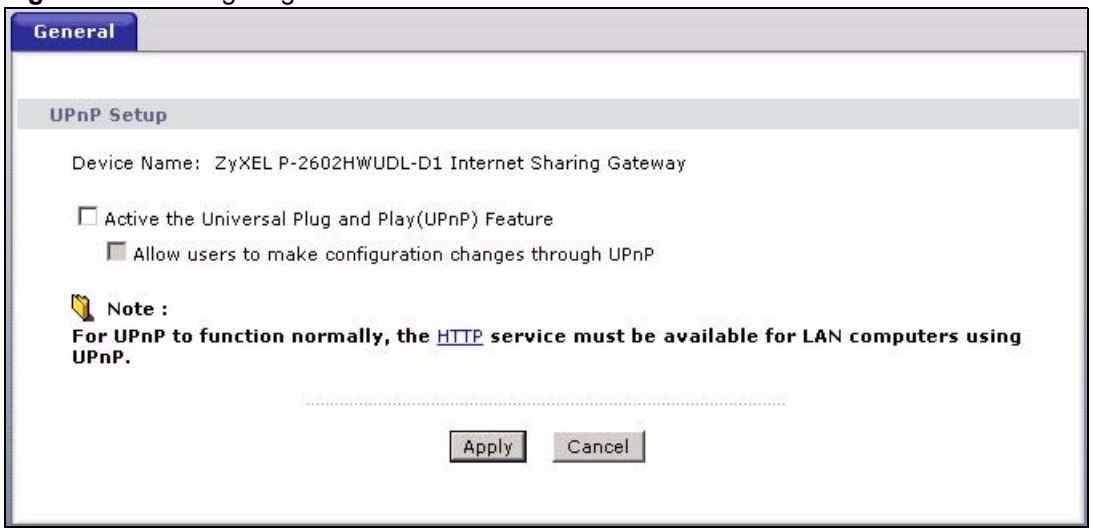
See the following sections for examples of installing and using UPnP.

24.2.1 Configuring UPnP

Click **Advanced > UPnP** to display the screen shown next.

See Section 24.1 on page 347 for more information.

Figure 238 Configuring UPnP


General
UPnP Setup
Device Name: ZyXEL P-2602HWUDL-D1 Internet Sharing Gateway
Active the Universal Plug and Play(UPnP) Feature
Allow users to make configuration changes through UPnP
Note :
For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Apply
Cancel

The following table describes the fields in this screen.

Table 132 Configuring UPnP

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Table 132 Configuring UPnP

LABEL	DESCRIPTION
Apply	Click **Apply** to save the setting to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previously saved settings.

24.3 Installing UPnP in Windows Example

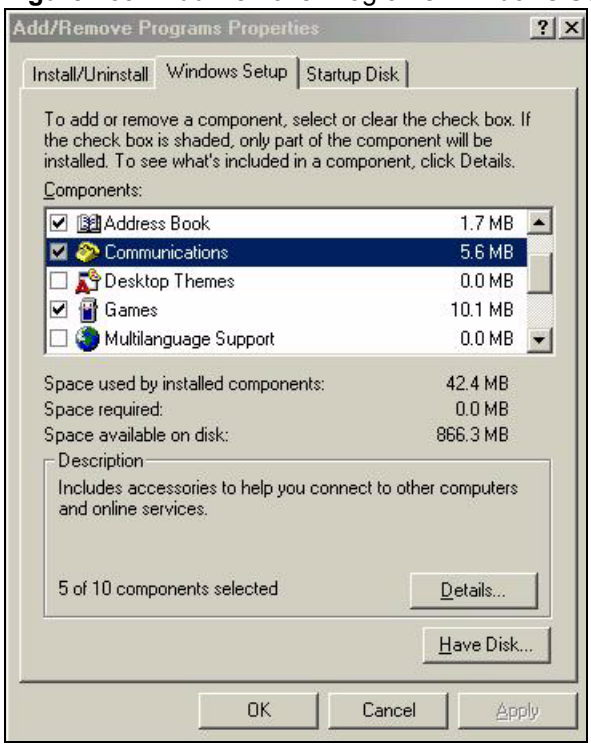
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

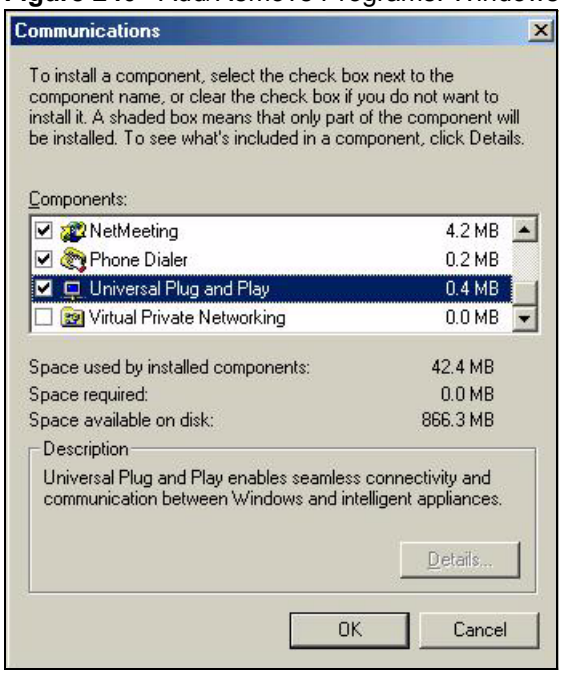
1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 239 Add/Remove Programs: Windows Setup: Communication


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 240 Add/Remove Programs: Windows Setup: Communication: Components


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

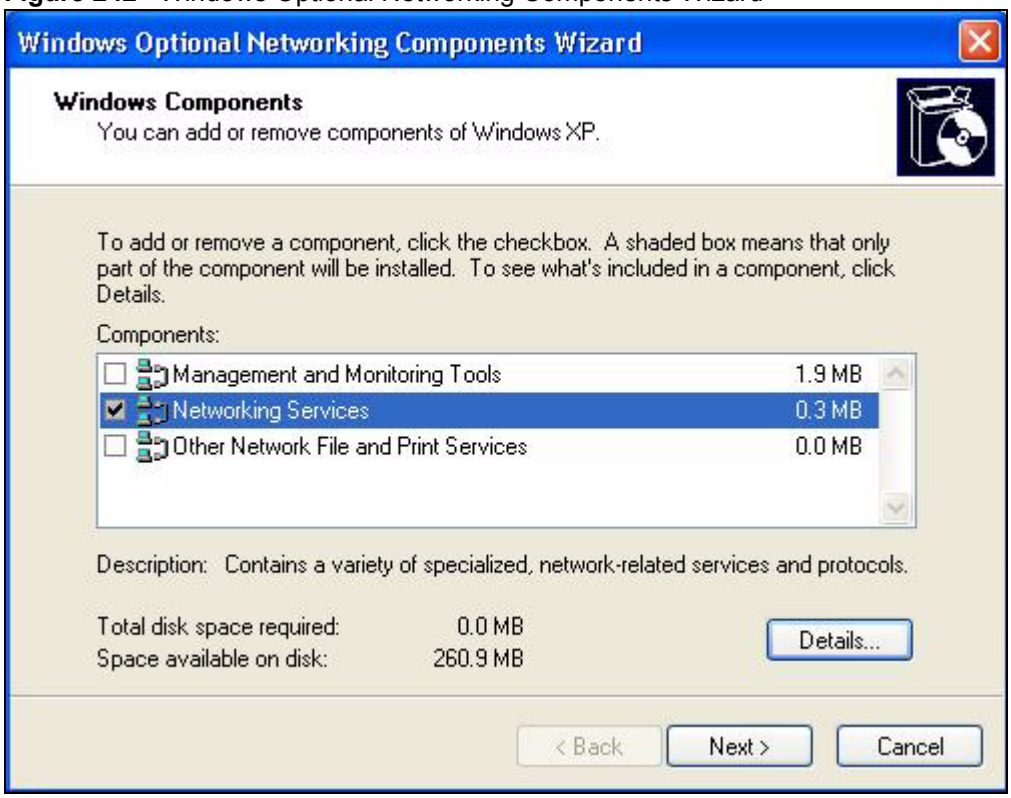
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 241 Network Connections

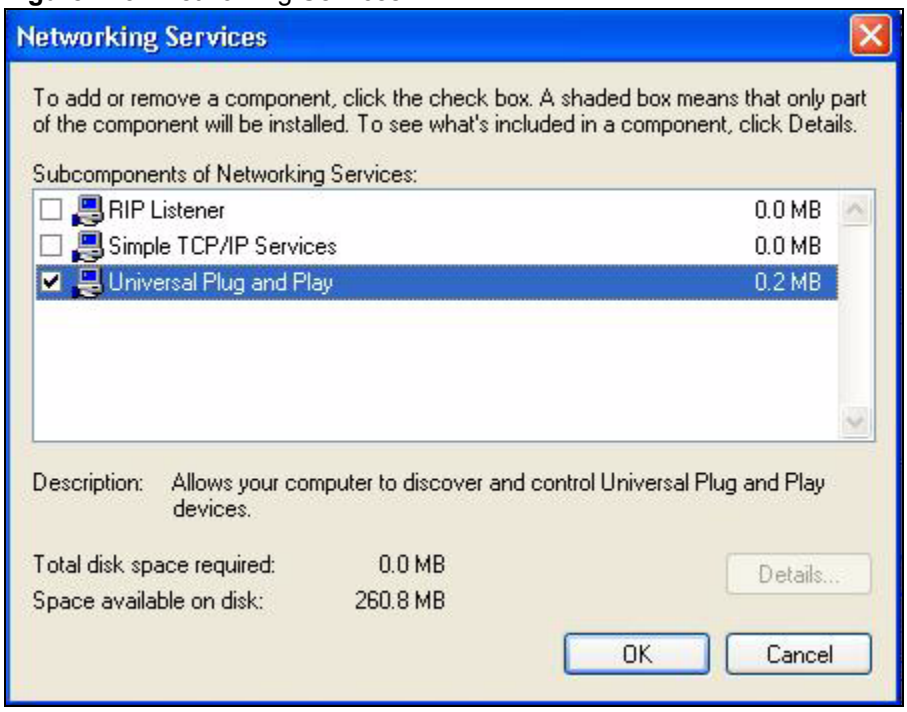
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 242 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 243 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

24.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
2. Right-click the icon and select **Properties**.

Figure 244 Network Connections

3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 245 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 246 Internet Connection Properties: Advanced Settings

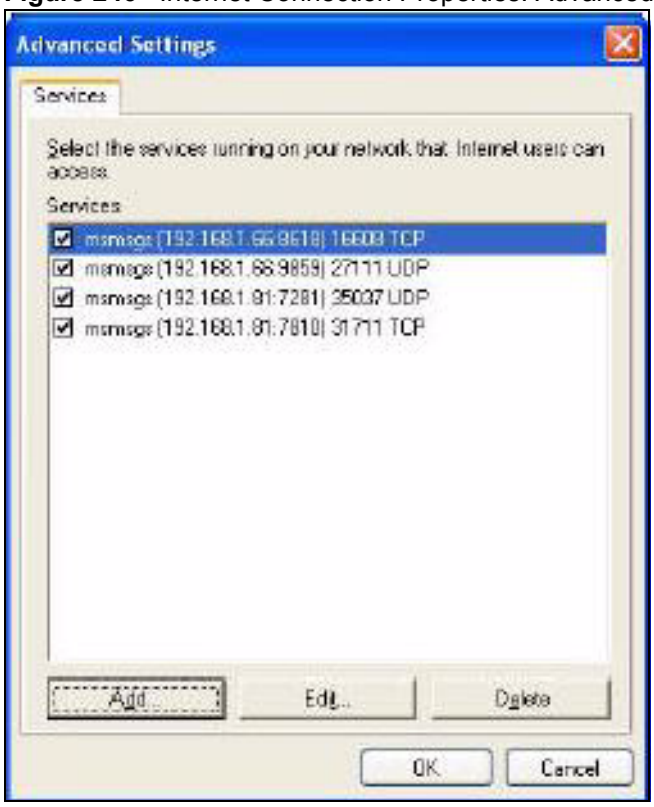
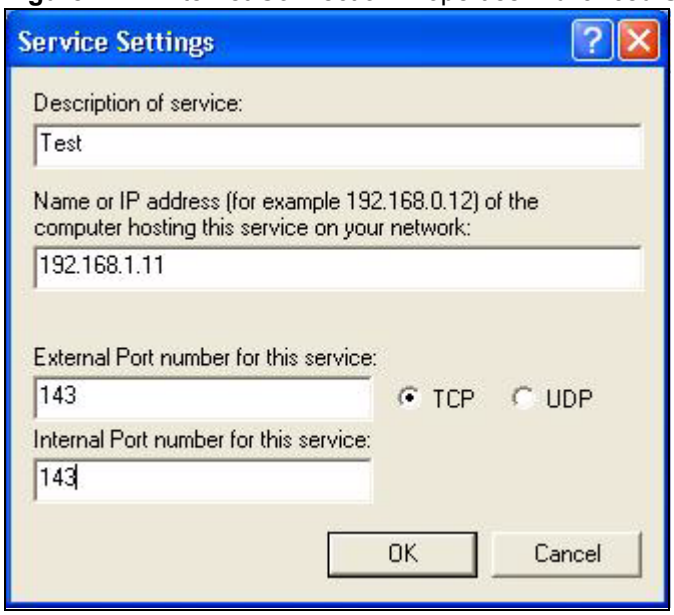


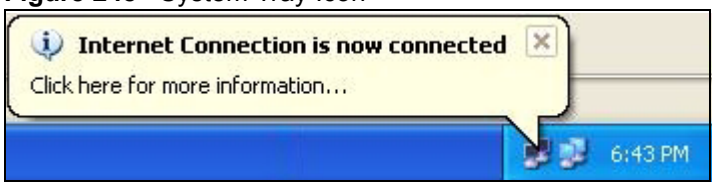
Figure 247 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 248 System Tray Icon



7 Double-click on the icon to display your current Internet connection status.

Figure 249 Internet Connection Status

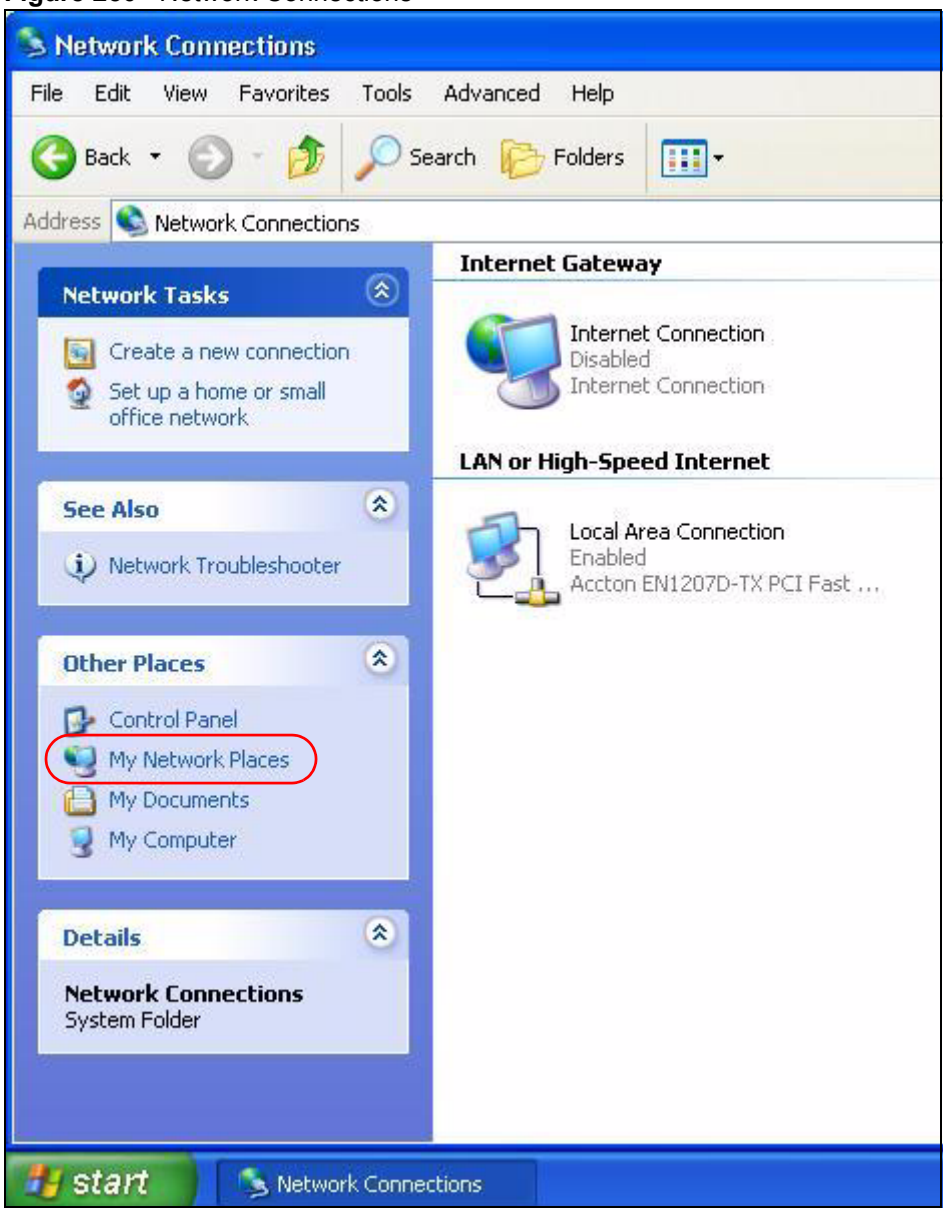
Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.
2 Double-click **Network Connections**.
3 Select **My Network Places** under **Other Places**.

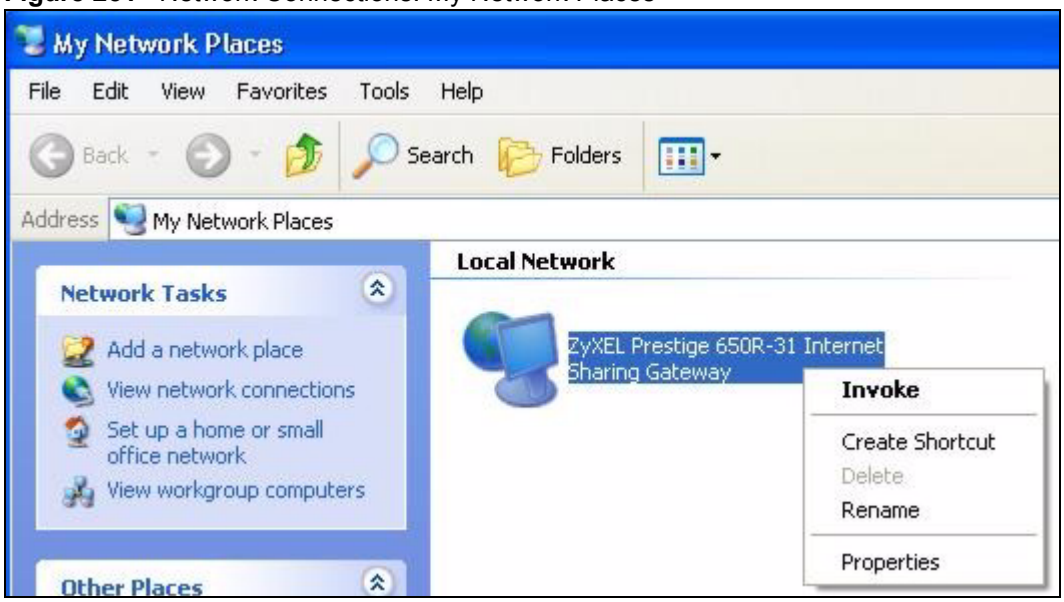
Figure 250 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 251 Network Connections: My Network Places



6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

Figure 252 Network Connections: My Network Places: Properties: Example

25

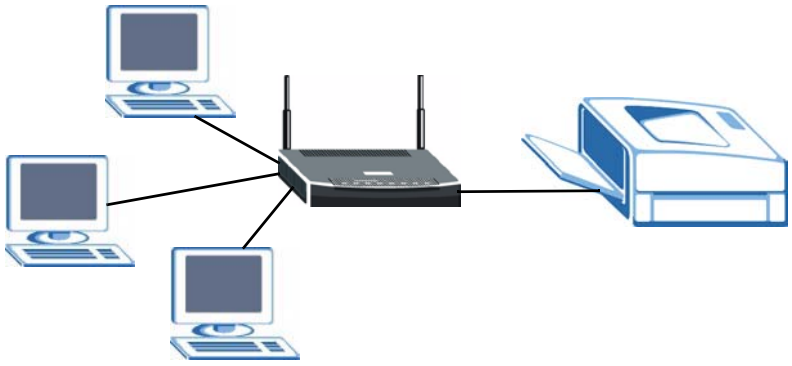
Sharing a USB Printer

This chapter describes how you can share a USB printer via your ZyXEL Device.

25.1 Overview

The ZyXEL Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the ZyXEL Device and then configuring a TCP/IP port on the computers connected to your network.

Figure 253 Sharing a USB Printer



The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer. See Section 25.5 on page 365 for an example of adding a printer.

25.2 Requirements

To configure the print server you need the following:

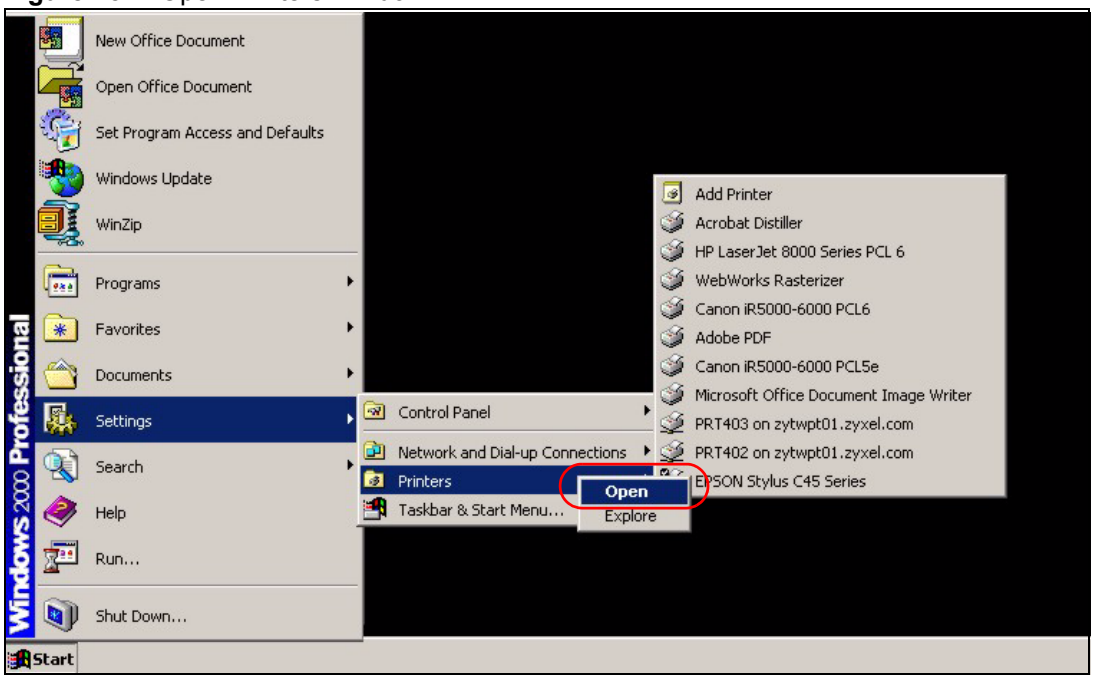
- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.
- Your operating system must support TCP/IP ports for printing and be compatible with the Line Printer Remote (LPR) protocol.
- A USB printer with the driver already installed on your computer.

25.3 Configure a TCP/IP Printer Port

This example shows screens from a Windows 2000 Professional operating system. Some menu items may look different on your system. The TCP/IP port must be configured with the IP address of the ZyXEL Device and must use the LPR (Line Printer Remote) protocol to communicate with the printer. Consult your operating systems documentation for instructions on how to do this or follow the instructions below if you have a Windows 2000/XP operating system.

1 Click **Start**, **Settings**, then right click on **Printers** and select **Open**.

Figure 254 Open Printers Window

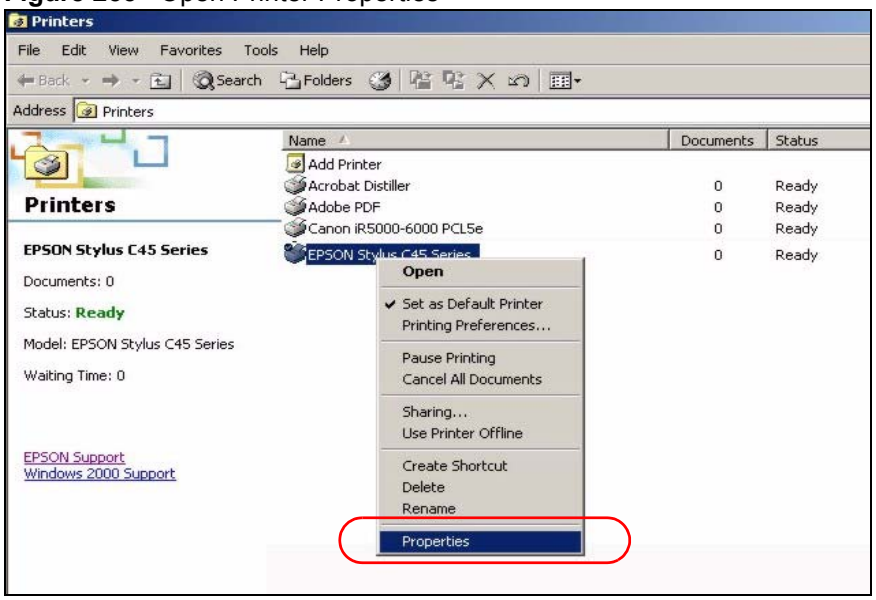


The **Printers** folder opens up. First you need to open up the properties windows for the printer you want to configure a TCP/IP port.

2 Locate your printer.

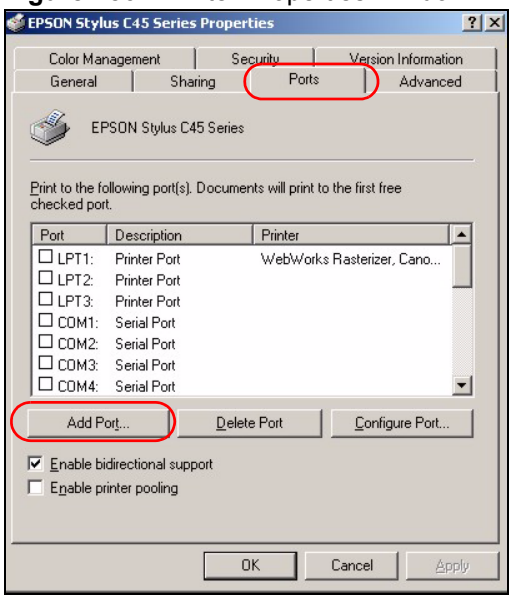
3 Right click on your printer and select properties.

Figure 255 Open Printer Properties



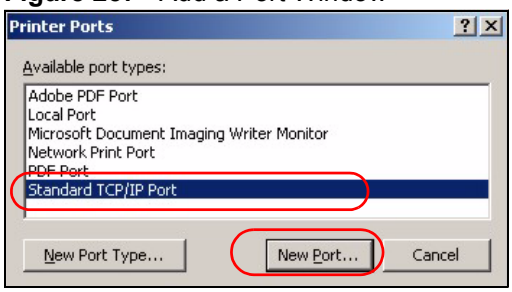
4 Select the **Ports** tab and click **Add Port...**

Figure 256 Printer Properties Window



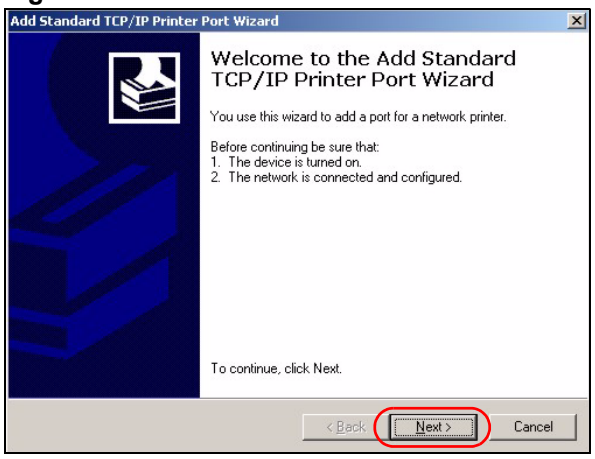
5 A **Printer Ports** window appears. Select **Standard TCP/IP Port** and click **New Port..**.

Figure 257 Add a Port Window



6 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

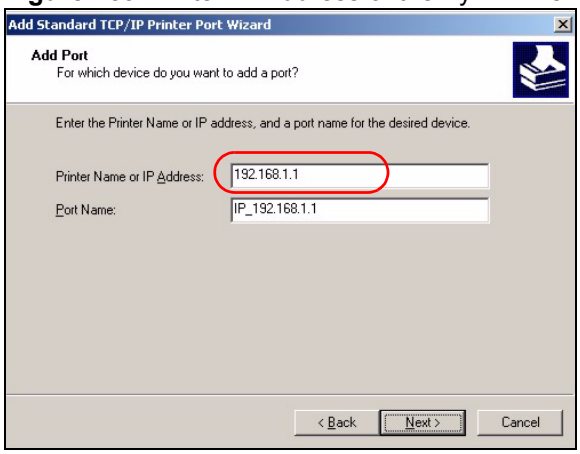
Figure 258 Add a Port Wizard


Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

7 Enter the IP address of the ZyXEL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ZyXEL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

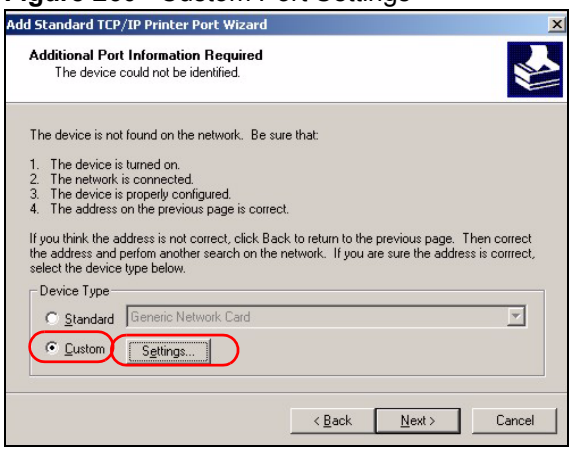
The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.

Figure 259 Enter IP Address of the ZyXEL Device


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

8 Select **Custom** under **Device Type** and click **Settings**.

Figure 260 Custom Port Settings

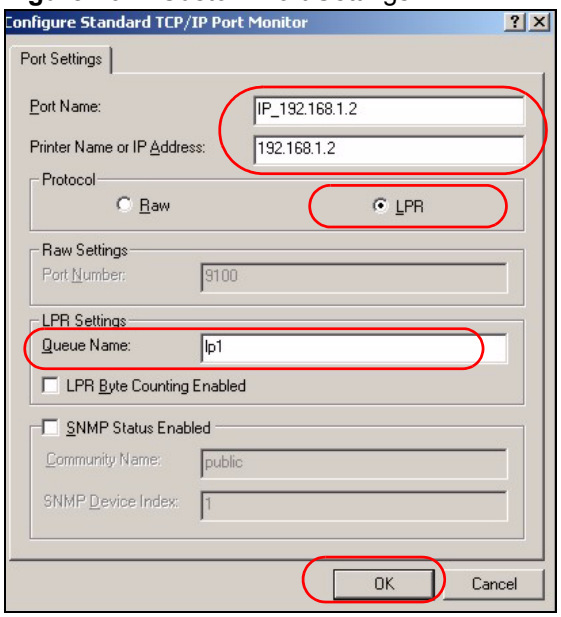

Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

9 Confirm the IP address of the ZyXEL Device in the IP Address field.

10 Select **LPR** under **Protocol**.

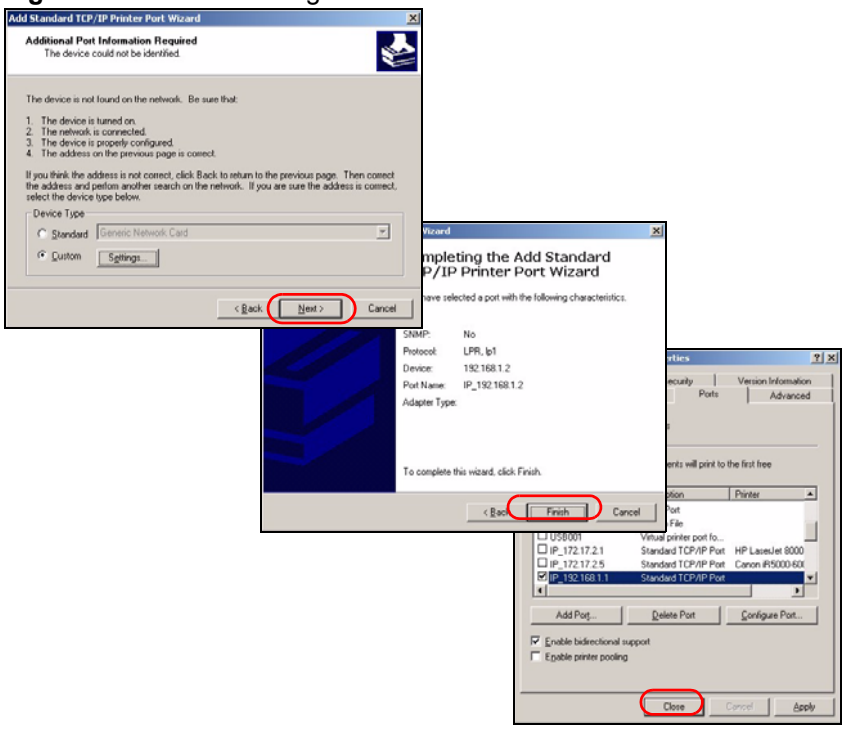
11 Type the LPR queue name of your printer model in the **Queue Name** field and click **OK**. Refer to your printer documentation for the LPR queue name. Some printer models accept any name you want to use, in this case you can enter a short descriptive name for the **Queue Name**.

Figure 261 Custom Port Settings



12 Continue through the wizard, apply your settings and close the wizard window.

Figure 262 Finish Adding the TCP/IP Port



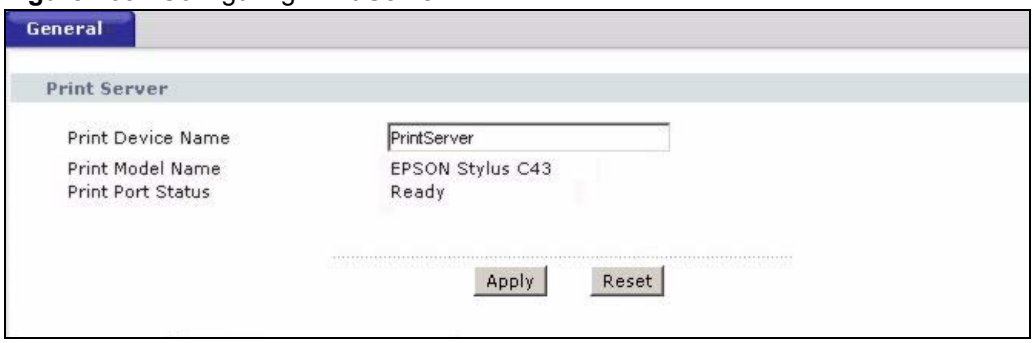
13 Repeat steps 1 to 12 to add this printer to other computers on your network.

25.4 Print Server Screen

The print server screen is used to confirm that the ZyXEL Device and the USB printer are able to communicate successfully.

Click **Advanced > Print Server** to display the **Print Server** screen.

Figure 263 Configuring Print Server



The following table describes the labels in this screen.

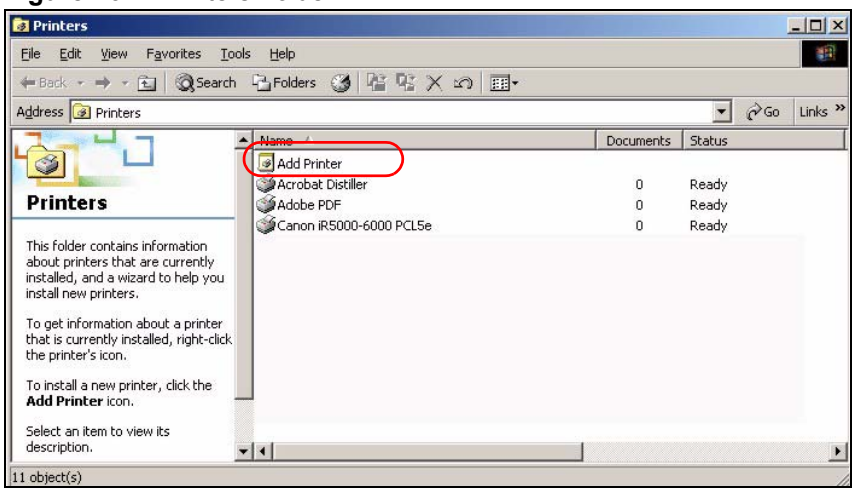
Table 133 Configuring Print Server

LABEL	DESCRIPTION
Print Device Name	Type a **Print Device Name** (of up to 31 printable characters) for recognition of the associated printer on the print server network. This name is displayed on a computer on the print server network when a print job is executed.
Print Model Name	This displays the model name of the printer currently connected to the ZyXEL Device print server.
Print Port Status	This field displays the print server status on the ZyXEL Device. **Ready**: The print server has established a TCP/IP connection with a printer, is online and ready to print. **Printing**: A computer on the print server network is executed a print job. **PaperOut**: The printer loading tray has no paper to perform the printing job **OFF LINE**: The computers in the print server network cannot use the print server. Make sure a USB v1.1 compliant printer is connected to the ZyXEL Device's USB port and powered on.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to configure the **Print Device Name** afresh.

25.5 Adding a New Printer Example

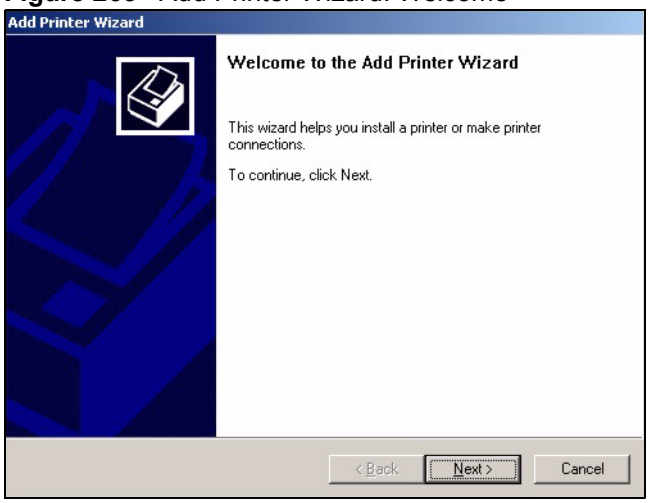
1 Open your **Printers** folder and double click **Add Printer**.

Figure 264 Printers Folder


Printers
File Edit View Favorites Tools Help
Back Search Folders
Address Printers
Go Links
Name
Documents
Status
Add Printer
Acrobat Distiller 0 Ready
Adobe PDF 0 Ready
Canon iR5000-6000 PCL5e 0 Ready
Printers
This folder contains information about printers that are currently installed, and a wizard to help you install new printers.
To get information about a printer that is currently installed, right-click the printer's icon.
To install a new printer, click the Add Printer icon.
Select an item to view its description.
11 object(s)

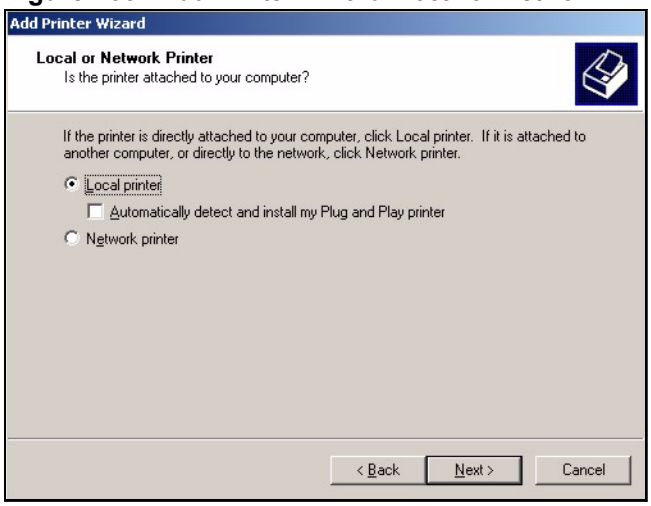
2 The **Add Printer Wizard** screen displays. Click **Next**.

Figure 265 Add Printer Wizard: Welcome


Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
To continue, click Next.
< Back
Next >
Cancel

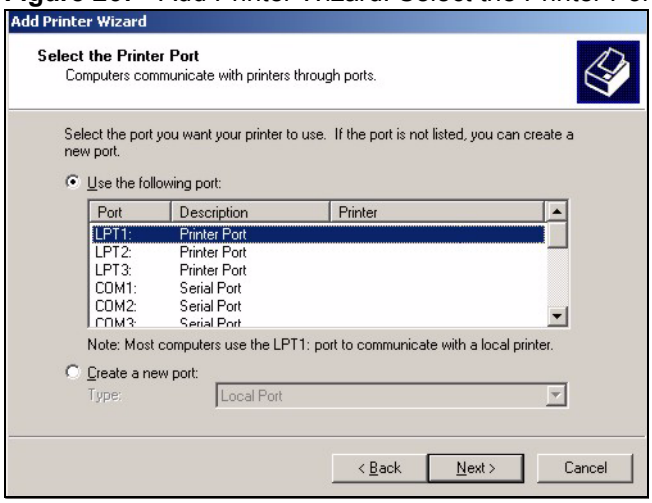
3 Select **Local printer** and click **Next**.

Figure 266 Add Printer Wizard: Local or Network Printer


Add Printer Wizard
Local or Network Printer
Is the printer attached to your computer?
If the printer is directly attached to your computer, click Local printer. If it is attached to another computer, or directly to the network, click Network printer.
Local printer
Automatically detect and install my Plug and Play printer
Network printer
< Back
Next >
Cancel

4 Select an **LPT** (Line Printing Terminal) port (a parallel port) as the computer interface for the USB printer.

Figure 267 Add Printer Wizard: Select the Printer Port



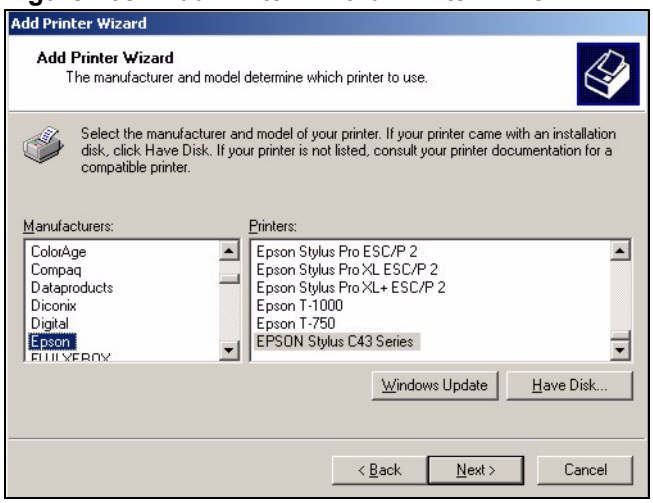
5 Select the make of the printer that you want to connect to the print server in the **Manufacturers** list of printers.

6 Select the printer model from the list of **Printers**.

7 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk…** and install the new printer driver.

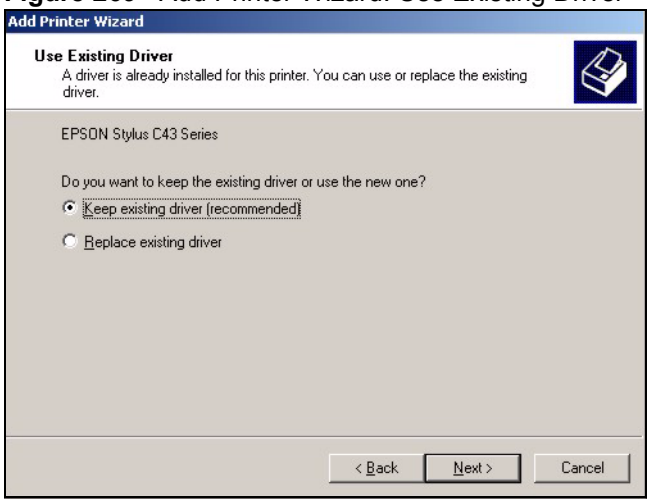
8 Click **Next** to continue.

Figure 268 Add Printer Wizard: Printer Driver


Add Printer Wizard
Add Printer Wizard
The manufacturer and model determine which printer to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.
Manufacturers:
Printers:
ColorAge
Compaq
Dataproducts
Diconix
Digital
Epson
Epson Stylus Pro ESC/P 2
Epson Stylus Pro XL ESC/P 2
Epson Stylus Pro XL+ ESC/P 2
Epson T-1000
Epson T-750
EPSON Stylus C43 Series
Windows Update
Have Disk...
< Back
Next >
Cancel

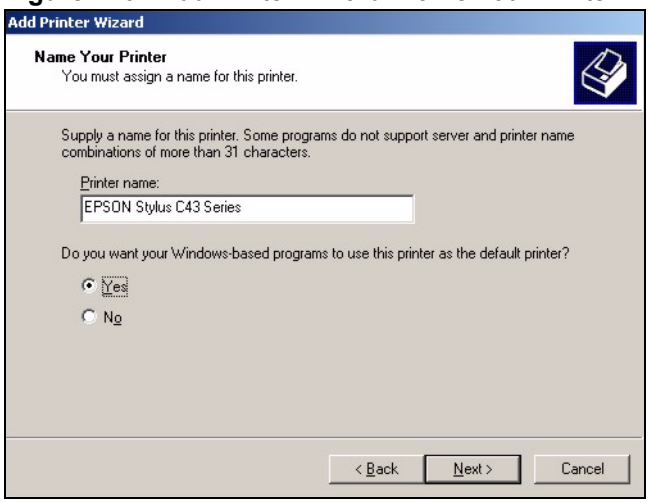
9 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.

Figure 269 Add Printer Wizard: Use Existing Driver


Add Printer Wizard
Use Existing Driver
A driver is already installed for this printer. You can use or replace the existing driver.
EPSON Stylus C43 Series
Do you want to keep the existing driver or use the new one?
Keep existing driver (recommended)
Replace existing driver
< Back
Next >
Cancel

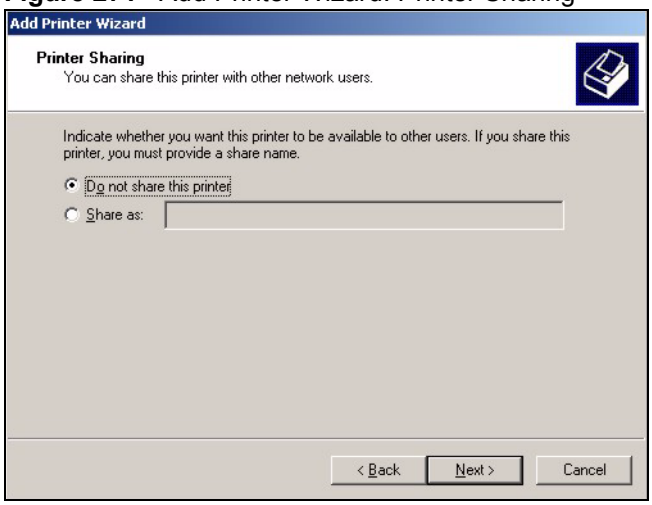
10 Type a name to identify the printer and then click **Next** to continue.

Figure 270 Add Printer Wizard: Name Your Printer


Add Printer Wizard
Name Your Printer
You must assign a name for this printer.
Supply a name for this printer. Some programs do not support server and printer name combinations of more than 31 characters.
Printer name:
EPSON Stylus C43 Series
Do you want your Windows-based programs to use this printer as the default printer?
Yes
No
< Back
Next >
Cancel

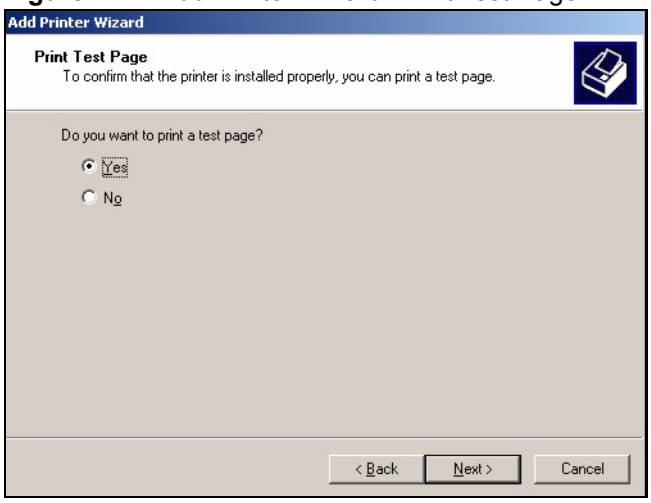
11 The ZyXEL Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same network; just select **Do not share this printer** and click **Next** to proceed to the following screen.

Figure 271 Add Printer Wizard: Printer Sharing


Add Printer Wizard
Printer Sharing
You can share this printer with other network users.
Indicate whether you want this printer to be available to other users. If you share this printer, you must provide a share name.
Do not share this printer
Share as:
< Back
Next >
Cancel

12 Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.

Figure 272 Add Printer Wizard: Print Test Page


Add Printer Wizard
Print Test Page
To confirm that the printer is installed properly, you can print a test page.
Do you want to print a test page?
Yes
No
< Back
Next >
Cancel

13 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.

Figure 273 Add Printer Wizard Complete

25.6 Macintosh OS X Adding Printer Example

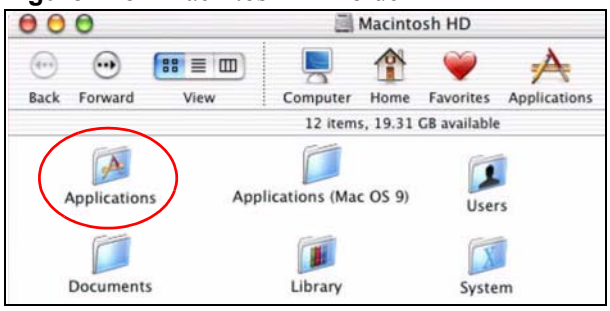
Use the following steps to set up a print server driver on your Macintosh computer.

1. Click the **Print Center** icon located in the Macintosh Dock (a place holding a series of icons/shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.
2. On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

Figure 274 Macintosh HD

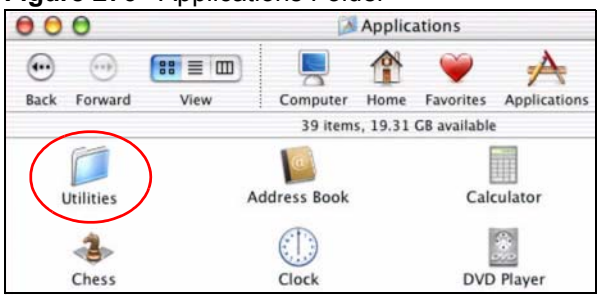
3. Double-click the **Applications** folder.

Figure 275 Macintosh HD folder



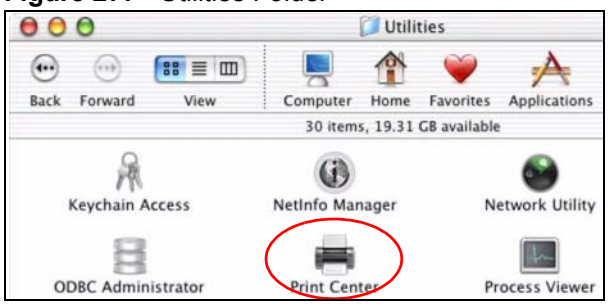
4. Double-click the **Utilities** folder.

Figure 276 Applications Folder



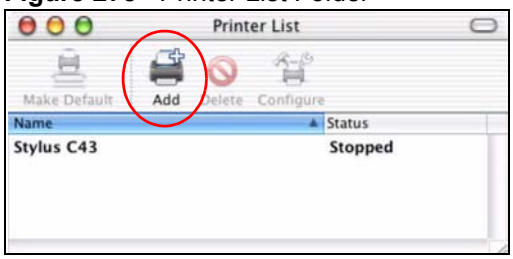
5 Double-click the **Print Center** icon.

Figure 277 Utilities Folder



6 Click the **Add** icon at the top of the screen.

Figure 278 Printer List Folder



7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

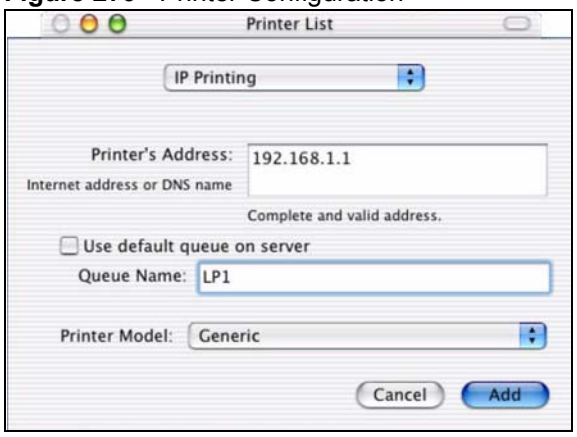
8 In the **Printer's Address** field, type the IP address of your ZyXEL Device.

9 Deselect the **Use default queue on server** check box.

10 Type **LP1** (a parallel port) in the **Queue Name** field.

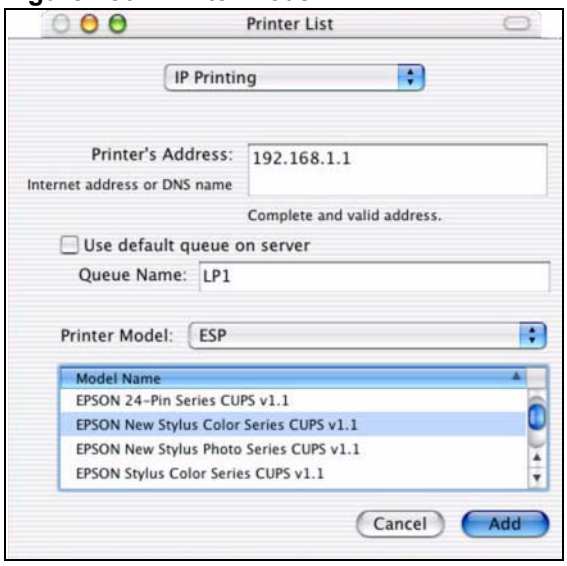
11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.

Figure 279 Printer Configuration



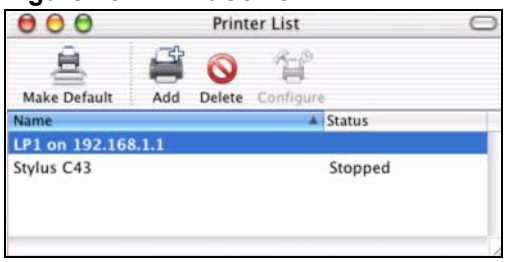
12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.

Figure 280 Printer Model



13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.

Figure 281 Print Server



14 Your Macintosh print server driver setup is complete. You can now use the ZyXEL Device's print server to print from a Macintosh computer.

25.7 ZyXEL Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the ZyXEL Device print server.

Table 134 Compatible USB Printers

BRAND	MODEL	BRAND	MODEL
Brother	HL1260	HP	Designjet 100
Brother	MFC4800	HP	Designjet 600
Brother	MFC4800J	HP	Designjet 650C
Brother	MFC6800	HP	Designjet 700
Brother	MFC7220	HP	Designjet 750C+
Brother	MFC7420	HP	LaserJet 1100
Brother	MFC8840D	HP	LaserJet 1160
CANON	S520	HP	LaserJet 1200
CANON	I6100	HP	LaserJet 1220
CANON	I6500	HP	LaserJet 1300
CANON	BJ-330	HP	LaserJet 1320
CANON	BJC4200	HP	LaserJet 2100
CANON	BJC4300	HP	LaserJet 2200
CANON	BJC4550	HP	LaserJet 2200D
CANON	BJC4650	HP	LaserJet 2300
CANON	PIXMA ip4000	HP	LaserJet 2410
Citizen	GSX230	HP	LaserJet 2420
DATAMAX	I-4208	HP	LaserJet 2500
DATAMAX	I-4308	HP	LaserJet 2550
DOCUJET	1610F	HP	LaserJet 3015
DOCUJET	UA1610	HP	LaserJet 3200
EPSON	C750	HP	LaserJet 3330
EPSON	LQ-100	HP	LaserJet 4000
EPSON	LQ-300	HP	LaserJet 4050
EPSON	LQ-300+	HP	LaserJet 4100
EPSON	LQ-570C	HP	LasetJet 4250
EPSON	LQ-1000C	HP	LasetJet 4300
EPSON	LQ-1170+	HP	LaserJet 4500
EPSON	LQ-1170C+	HP	LasetJet 4650

Table 134 Compatible USB Printers (continued)

BRAND	MODEL	BRAND	MODEL
EPSON	LQ-1170C	HP	LasetJet 5000
EPSON	LQ-2070C	HP	LasetJet 5000LE
EPSON	LQ-2080C	HP	LasetJet 5100LE
EPSON	LQ-2090	HP	LaserJet 6P
EPSON	LQ-2170C	HP	LaserJet 8100
EPSON	LQ-2180C	HP	OfficeJet K850
EPSON	LQ-2550	IBM	Infoprint 20
EPSON	LQ-3500C	IBM	Infoprint 1116
EPSON	LQ-670	IBM	Infoprint 1312
EPSON	LQ-680	IBM	Infoprint 1316
EPSON	LQ-680C	IBM	Infoprint 1332
EPSON	STYLUS C60	IBM	Infoprint 1412
EPSON	Stylus C63	Konica Minolta	DI 152
EPSON	Stylus C67	Konica Minolta	DI 250
EPSON	Stylus C83	Konica Minolta	Pagepro 1300W
EPSON	Stylus Color 400	Konica Minolta	Pagepro 1350W
EPSON	Stylus Color 600	Konica Minolta	Magicolor 2450
EPSON	Stylus Color 670	Konica Minolta	Magicolor 5450
EPSON	Stylus Color 800	Kyocera	FS-1010
EPSON	Stylus Color 810	Kyocera	FS-1020
EPSON	Stylus Color 850	Kyocera	FS-1920
EPSON	Stylus Pro 7600	Kyocera	FS-720
EPSON	Stylus Photo 1270	Kyocera	FS-820
EPSON	Stylus Photo 810	Kyocera	FS-920
EPSON	Stylus Photo 900	Kyocera	FS-6020
EPSON	Stylus Photo EX2	LEXMARK	E210
EPSON	Stylus Photo EX3	LEXMARK	E322
EPSON	Stylus Photo R1800	LEXMARK	Optra S1250
EPSON	ACULASER C1900	LEXMARK	T420
EPSON	EPL5700	LEXMARK	T620

Table 134 Compatible USB Printers (continued)

BRAND	MODEL	BRAND	MODEL
EPSON	EPL5800	LEXMARK	C720
EPSON	EPL5900	LEXMARK	C750
EPSON	EPL6100	LEXMARK	W812
EPSON	EPL6200	LEXMARK	Z43
EPSON	EPL-N2120	LEXMARK	Z55
EPSON	TM T88III	LEXMARK	Z705
FUJITSU	DL-700	LEXMARK	Z515
FUJITSU	DL-900	MITAC	MP-6600C
FUJITSU	DL-3400	NEC	Pinwriter P2200
FUJITSU	DL-3800	NEC	Pinwriter P3200
FUJITSU	DL-3850	NEC	Pinwriter P5300
FUJITSU	DL-5800	NEC	Pinwriter P8000C
FUJITSU	DL-6400Pro	OKI	Microline 391
FUJITSU	DL-6800	OKI	B4350
FUJITSU	FP 410	RICOH	NF3570
FUJITSU	Jet Wind 500C	PANASONIC	KX-P1121
FUJITSU	PP 10	PANASONIC	KX-P1123
FUTEK	F8000	PANASONIC	KX-P1124
FUTEK	F84+	PANASONIC	KX-P1624
FUTEK	F86+	PANASONIC	KX-P6500
HP	Color Laserjet 2605	SAMSUNG	ML-1710
HP	Color Laserjet 3700	SAMSUNG	ML-1750
HP	DeskJet 400	SAMSUNG	ML-2250
HP	DeskJet 450C	SAMSUNG	ML-2550
HP	DeskJet 500	SAMSUNG	CLP 500
HP	DeskJet 670C	SAMSUNG	CLP 510
HP	DeskJet 680C	SAMSUNG	SRP 270
HP	DeskJet 720C	SAMSUNG	SCX-4016
HP	DeskJet 810C	SAMSUNG	SCX-4100
HP	DeskJet 830C	Sharp	AR-255

Table 134 Compatible USB Printers (continued)

BRAND	MODEL	BRAND	MODEL
HP	DeskJet 920C	Sharp	AR-265FG
HP	DeskJet 930C	Sharp	AR-M 160
HP	DeskJet 948C	Sharp	AR-M 205
HP	DeskJet 970CXI	Sharp	AR-M 207
HP	DeskJet 1120C	Sharp	AR-M 235
HP	DeskJet 1125C	Sharp	AR-M 275
HP	DeskJet 1180C	Sharp	AR-M 350
HP	DeskJet 1280	Sharp	AR-M 400
HP	DeskJet 3820	Sharp	AR-M 450
HP	DeskJet 5500	STAR	NX-2420
HP	DeskJet 5550	TOSHIBA	E-161
HP	DeskJet 5652	TOSHIBA	Estudio-25
HP	DeskJet 9300	XEROX	Phaser 3310
HP	DeskJet 9600	XEROX	Able 3321
HP	DeskJet 9650	XEROX	Docuprint 240A
HP	DeskJet 9800		

26

File Sharing

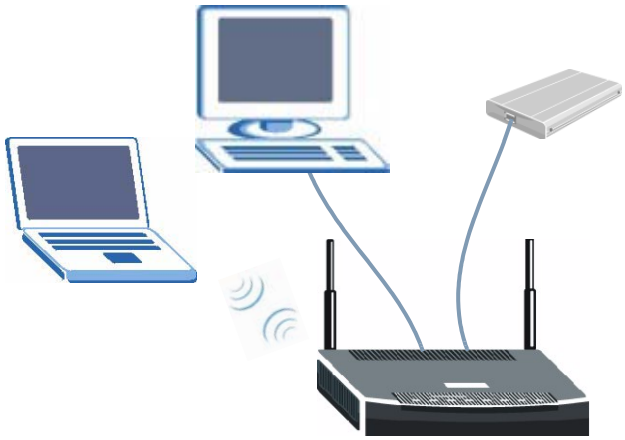
Use these screens to set up file sharing through your ZyXEL Device.

26.1 File Sharing Implementation Overview

Your ZyXEL Device allows you to connect USB 2.0 (or lower) file storage devices so that they can be accessed by users connected to your network. A file storage device can be a USB memory stick or a hard drive with a USB connector. The following figure is an overview of the ZyXEL Device's file server feature.

File Allocation Table (FAT) and FAT32 file systems are the only file systems compatible with the file sharing feature.

Figure 282 File Sharing Overview



Do the following to set up file sharing via your ZyXEL Device:

Before connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

1. Connect a USB memory stick (or a USB hard drive) to one of the ZyXEL Device's USB ports.
2. The ZyXEL Device detects the USB device and makes its contents available for browsing. If your USB device cannot be detected by ZyXEL Device, see the troubleshooting suggestions for The ZyXEL Device fails to detect my USB device. If you connect more than one device (or your hard drive has more than one partition), each device (or partition) is given its own folder. These folders are called "shares".
3. Configure a user account. Anyone who wants to access your shared files must enter a user name and password. See Section 26.3 on page 379 for more information.

26.2 Sharing Files via the ZyXEL Device

The ZyXEL Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility). CIFS compatible computers can access the USB file storage devices connected to the ZyXEL Device.

26.2.1 Using the Workgroup Name to Share Files

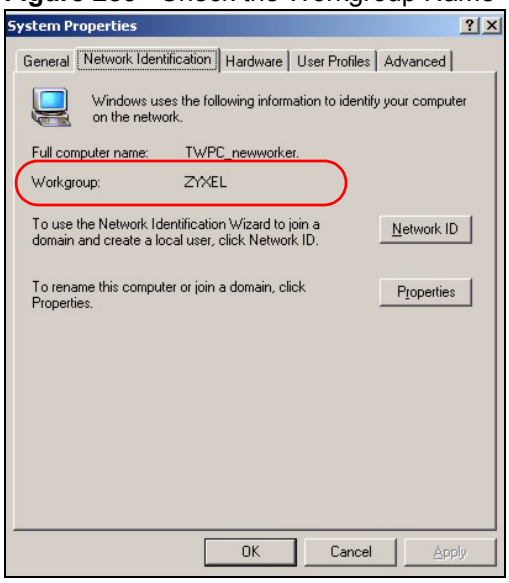
In order to use this method to share files you need to add the ZyXEL Device to the workgroup on the network to which your computer belongs. In a typical home network this workgroup name is "Workgroup".

The ZyXEL Device will not be accessible via the workgroup name if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

26.2.1.1 Checking your Workgroup Name

You can check the name of the workgroup to which your computer belongs by viewing the **Network Identification** information of your Windows 2000 computer. Click **Start > Settings > Control Panel > System**. Select the **Network Identification** tab and note the workgroup name of your computer. This is the value you have to enter in the **Workgroup Name** field in the **File Sharing** screen.

Figure 283 Check the Workgroup Name



26.3 User Accounts

The ZyXEL Device requires that a user enter a user name and password in order to access files on the USB storage device. When you browse to the ZyXEL Device you are prompted for a user name and password before you can access files on the USB storage device.

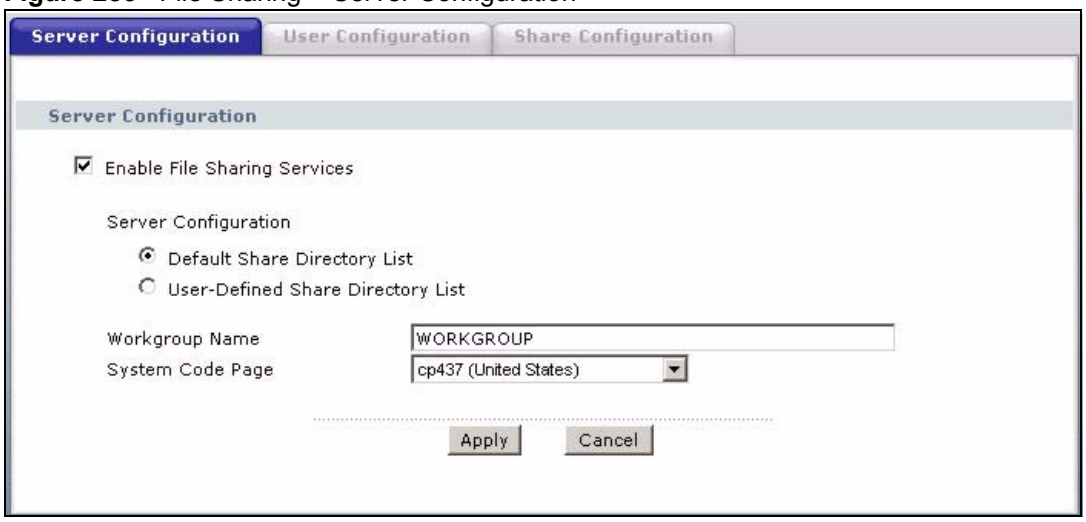
Figure 284 File Sharing Login

Once logged in, you do not have to re-login until you restart the computer, even if the administrator changes the username and password.

26.4 File Sharing - Server Configuration

Use this screen to set up file sharing via the ZyXEL Device. To access this screen, click **Advanced > File Sharing**.

Figure 285 File Sharing > Server Configuration



Each field is described in the following table.

Table 135 File Sharing > Server Configuration

LABEL	DESCRIPTION
Enable File Sharing Services	Select this to enable file sharing through the ZyXEL Device.
Server Configuration	Select **Default Share Directory List** to use the preset share names. Select **User-Defined Share Directory List** to use your own share names and set access levels.
Workgroup Name	You can add the ZyXEL Device to an existing workgroup on your network Type the name of an existing workgroup on your network. The ZyXEL Device automatically joins this workgroup and you can browse to it via Windows Explorer. See Section 26.2.1 on page 378 for more information. Note: If the workgroup name is not entered exactly the same as the workgroup name to which your computer belongs to, browsing via the network neighborhood will not work.
System Code Page	Select the character set of the files contained on your storage device. For example, if your files were created on an operating system which used the Russian alphabet, select **cp866 (Russian)**. If the file or folder names on your USB storage device appear as unrecognizable (or jumbled) characters, you should double check this setting to make sure it is set correctly.
Apply	Click this to save your changes to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

26.5 User Configuration

Use this screen to configure a user account. To access this screen, click **Advanced > File Sharing > User Configuration**.

Figure 286 File Sharing > User Configuration

Each field is described in the following table.

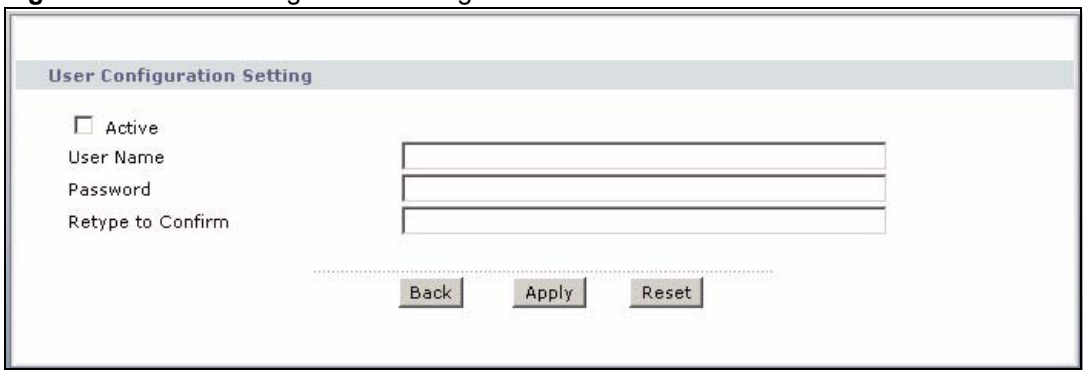
Table 136 File Sharing > User Configuration

LABEL	DESCRIPTION
#	This is a read-only index number of the user name on the ZyXEL Device.
Active	This shows whether the user name is active (able to access shares via the ZyXEL Device) or inactive (unable to access shares via the ZyXEL Device).
User Name	This field shows the list of user names already configured on the ZyXEL Device.
Modify	Click the Edit icon to change the settings of an existing user account. Click the Remove icon to delete this entry in the list.
Add	Click this button to configure another user name and include it in the list.

26.5.1 Add or Edit a User Account

Use this screen to add or edit a user account. To access this screen, click **Advanced > File Sharing > User Configuration** and click the **Edit** icon in the **Modify** column or the **Add** button.

Figure 287 File Sharing > User Configuration > Add/Edit



Each field is described in the following table.

Table 137 File Sharing > User Configuration > Add/Edit

LABEL	DESCRIPTION
Active	Select this to set whether the user name is active (able to access shares via the ZyXEL Device) or inactive (unable to access shares via the ZyXEL Device).
User Name	This field is not configurable if you click the **Edit** icon in the **Modify** column to configure an existing user account. Enter the user name of the account. The user name can be 31 alpha-numeric characters long.

Table 137 File Sharing > User Configuration > Add/Edit

LABEL	DESCRIPTION
Password	Enter the password for this account. The password can be 31 alpha-numeric characters long.
Retype to Confirm	Retype the password.
Back	Click this button to return to the previous screen without saving your settings.
Apply	Click this to save your changes to the ZyXEL Device.
Cancel	Click this to set the fields in this screen to their defaults.

26.6 Share Configuration

Use this screen to configure a share name and directory. To access this screen, click **Advanced > File Sharing > Share Configuration**. The screen varies depending on whether you select to use the **Default Share Directory List** or **User-Defined Share Directory List** in the **Server Configuration** screen.

26.6.1 Default Share Directory List

Figure 288 File Sharing > Share Configuration: Default

Each field is described in the following table.

Table 138 File Sharing > Share Configuration: Default

LABEL	DESCRIPTION
Default Share Directory List	These fields identify the default shares on the ZyXEL Device.
#	This is a read-only index number of the default share on the ZyXEL Device. When more than one USB disk (or a USB hard drive with multiple shares) is connected to the ZyXEL Device this index number identifies the different disks. The first disk connected is 1, the second 2 and so on.
Share Name	This field displays the default share names on the ZyXEL Device. **usbdisk1** refers to the share name of the first USB memory disk connected to the ZyXEL Device, **usbdisk2** refers to the second USB memory disk connected to the ZyXEL Device and so on.
Share Directory	This field displays the share directories (folders) on the ZyXEL Device. These are the directories (folders) you can enter when you browse to your USB storage device.

26.6.2 User-Defined Share Directory List

Figure 289 File Sharing > Share Configuration: User-Defined

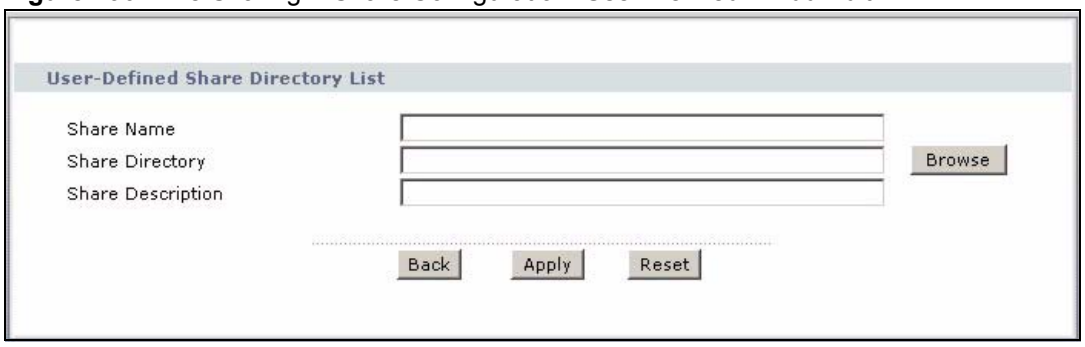
Each field is described in the following table.

Table 139 File Sharing > Share Configuration: User-Defined

LABEL	DESCRIPTION
User-Defined Share Directory List	These fields identify the shares you configured on the ZyXEL Device.
#	This is a read-only index number of the user-defined share on the ZyXEL Device.
Share Name	This field displays the user-defined share name on the ZyXEL Device.
Share Directory	This field displays the user-defined share directories (folders) on the ZyXEL Device. These are the directories (folders) you can enter when you browse to your USB storage device.
Share Description	This field displays information about the share. You can add share descriptions to user-defined shares in the **Share Configuration Add/Edit** screen.
Modify	Click the Edit icon to change the settings of an existing user-defined share. Click the Remove icon to delete this share in the list.
Add	Click this to set up a new user-defined share on the ZyXEL Device.

26.6.3 Add or Edit a User-Defined Share

Figure 290 File Sharing > Share Configuration: User-Defined > Add/Edit



Each field is described in the following table.

Table 140 File Sharing > Share Configuration: User-Defined > Add/Edit

LABEL	DESCRIPTION
Share Name	Enter the name you want the user-defined share to have in the network.
Share Directory	Manually enter the file path for the user-defined share, or click the **Browse** button.

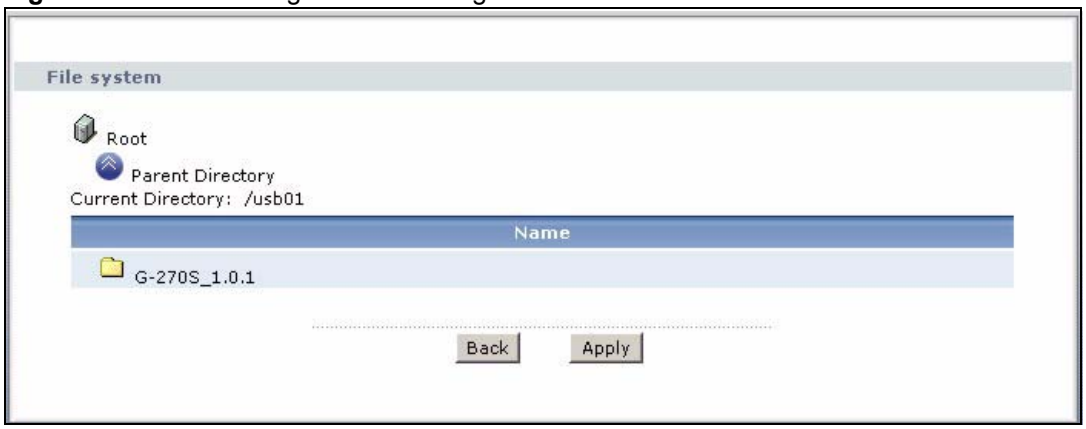
Table 140 File Sharing > Share Configuration: User-Defined > Add/Edit

LABEL	DESCRIPTION
Browse	Click this button to select the file path for the user-defined share directory. This is the folder that will be visible to a user browsing to the USB storage device. A user can access any files and sub-folders in this folder.
Share Description	You can either enter a short description of the share, or leave this field blank.
Back	Click this button to return to the previous screen without saving your settings.
Apply	Click this button to save your settings.
Reset	Click this button to return all fields in this screen to their default values.

26.6.4 Browse

To select the file path for the user-defined share directory, click **Browse** in the **Share Configuration Add/Edit** screen.

Figure 291 File Sharing > Share Configuration: User-Defined > Browse



Each field is described in the following table.

Table 141 File Sharing > Share Configuration: User-Defined > Browse

LABEL	DESCRIPTION
File System	Use this section to set up the directory path for the share.
Parent Directory	Click the **Parent Directory** icon ( ) to go up one level.
Current Directory	This field displays the file path of the share. This is the folder that will be visible to a user browsing to the USB storage device. A user can access any files and sub-folders in this folder.
Name	This displays the name of the folder in the **Current Directory** of the connected USB storage device. Click on a folder name to add that folder to the directory path for the share
Back	Click this button to return to the previous screen without saving your settings.
Apply	Click this button to save your settings.

26.7 Examples of Accessing Files via the ZyXEL Device

Once you have enabled file sharing and configured a user account for file sharing. The USB file storage devices become a part of your file structure. There are several ways to start browsing the file storage devices connected to the ZyXEL Device.

The examples in this User's Guide show you how to use Microsoft's Windows 2000 to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

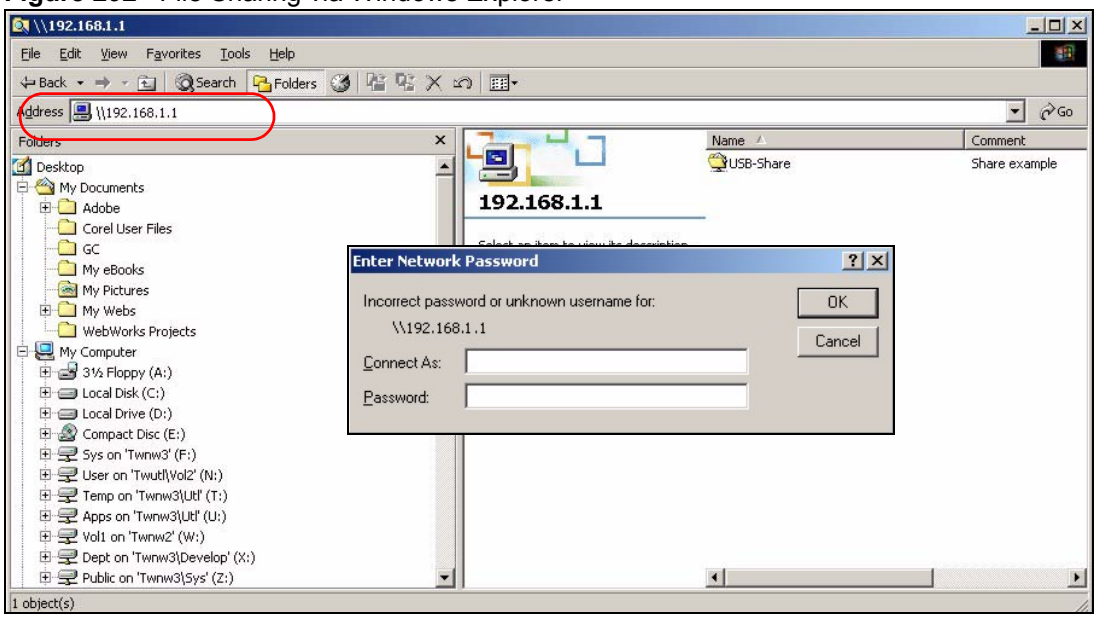
26.7.1 Using Windows Explorer to Share Files

CIFS protocol allows you to use the Windows Explorer to connect to the ZyXEL Device and access the file storage devices connected to it.

In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the ZyXEL Device (the default IP address of the ZyXEL Device is 192.168.1.1) and hit [ENTER]. A screen asking for password authentication appears. Enter the user name and password and hit **OK**. See Figure 292 on page 385.

Once you login to the file "share" via your ZyXEL Device, you do not have to relogin until you restart your computer.

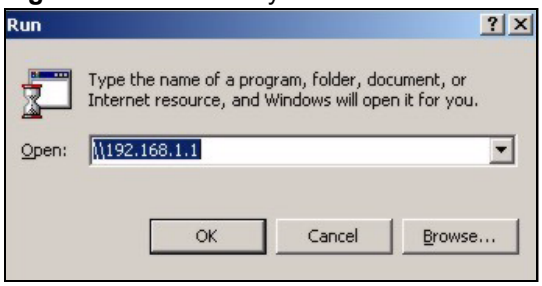
Figure 292 File Sharing via Windows Explorer



26.7.2 Using the Run Utility to Share Files

On your Windows 2000 computer, click **Start**, **Run** and type a double backslash "\\" followed by the IP address of the ZyXEL Device and click **OK**.

Figure 293 Run Utility to Browse Files



The **Run** utility automatically opens Windows Explorer and displays the contents of the USB storage device connected to your ZyXEL Device.

26.7.3 Using FTP to Share Files

You can use an FTP client to connect to the ZyXEL Device either from the LAN or the WAN and access the file storage devices connected to it.

In this example, we use the web browser to share files via FTP from the LAN. The way or screen you log into the FTP server (on the ZyXEL Device) varies depending on your FTP client. See your FTP client documentation for more information.

In your web browser's address or URL bar type "ftp:\\" followed by the IP address of the ZyXEL Device (the default LAN IP address of the ZyXEL Device is 192.168.1.1) and click **Go** or press [ENTER].

Figure 294 File Sharing via FTP: Address

ZyXEL Information Web - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address ftp://192.168.1.1
Go Links

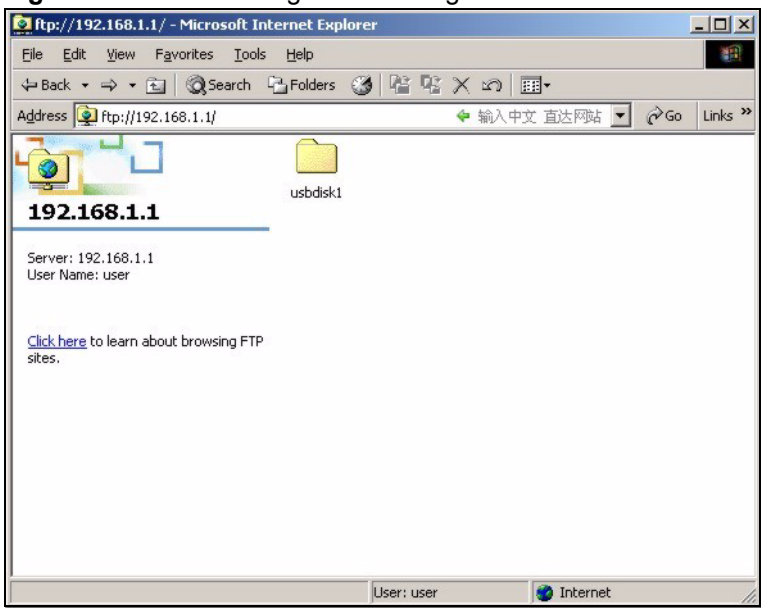
A screen asking for password authentication appears. Enter the user name and password (you configured in the **File Sharing** screen) and click **Login**.

Figure 295 File Sharing via FTP: Login

Login As
Either the server does not allow anonymous logins or the e-mail address was not accepted.
FTP Server: 192.168.1.1
User Name: user
Password: ********
After you login, you can return to this FTP server easily by adding it to your Favorites List.
Login Anonymously
Save Password
Login
Cancel

The screen changes and shows you the folder for the USB storage device connected to your ZyXEL Device. Double-click the folder to display the contents in it.

Figure 296 File Sharing via FTP: Login



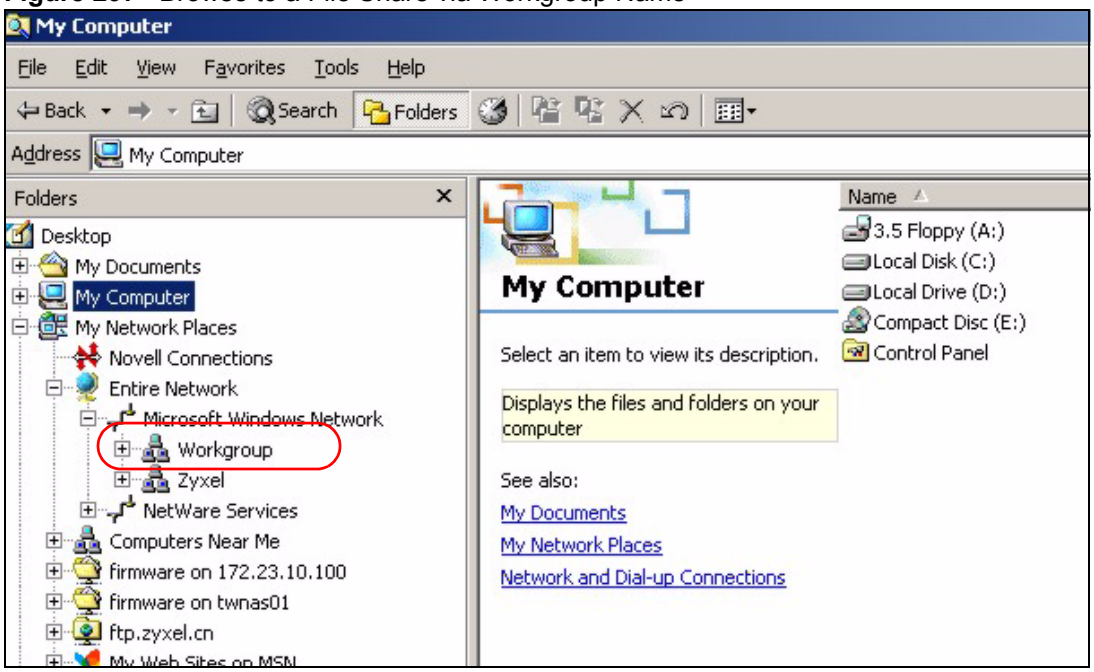
26.7.4 Using the Workgroup Name to Access Files

Before using this method to access files you need to make sure that you have correctly configured the workgroup name in the **File Sharing > General** screen. See Section 26.2.1 on page 378 for more information.

The ZyXEL Device will not be accessible via the workgroup name if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

Once the ZyXEL Device is a member of your workgroup, use Windows Explorer to browse to the file “share” by locating the workgroup in your file system. It is located under **My Network Places**. In our example the workgroup name is the default “Workgroup”.

Figure 297 Browse to a File Share via Workgroup Name



PART IV
Maintenance, Troubleshooting and Specifications

System (391)
Logs (395)
Tools (409)
Diagnostic (421)
Troubleshooting (425)
Product Specifications (433)

27

System

Use this screen to configure the ZyXEL Device's time and date settings.

27.1 General Setup and System Name

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

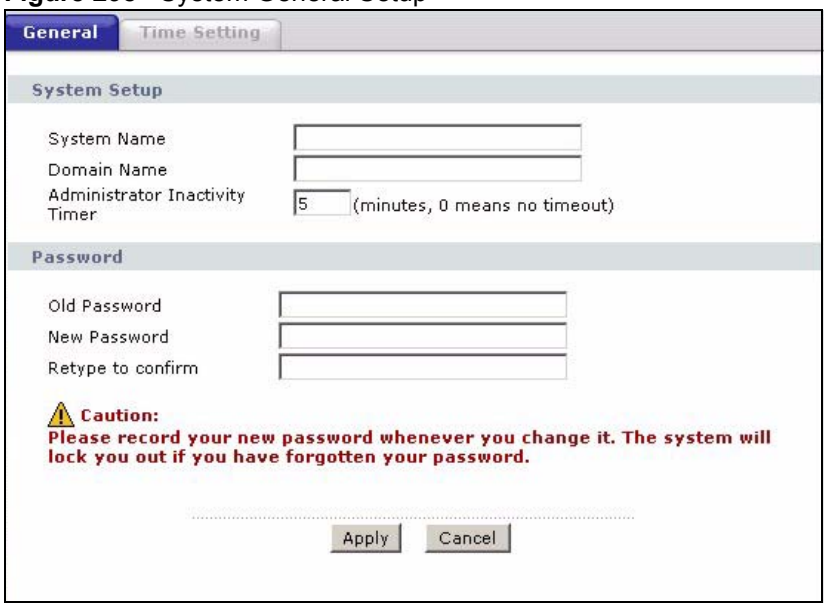
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

27.1.1 General Setup

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyXEL Device via DHCP.

Click **Maintenance > System** to open the **General** screen.

Figure 298 System General Setup



The following table describes the labels in this screen.

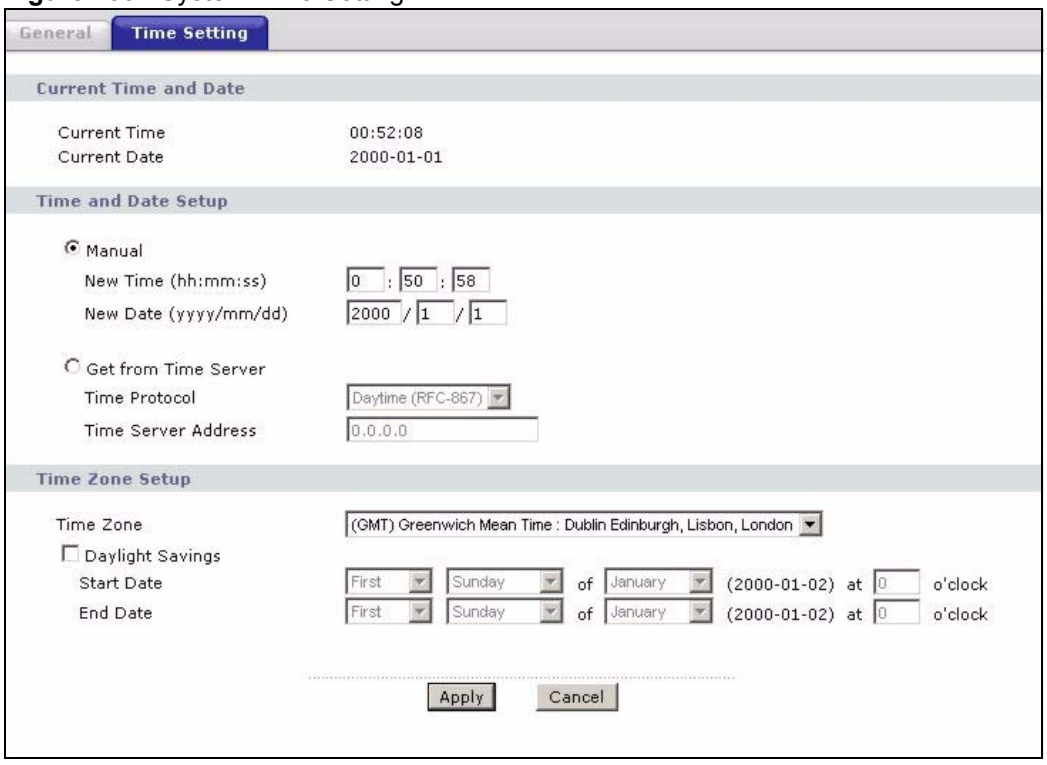
Table 142 System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or telnet) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password	
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

27.2 Time Setting

To change your ZyXEL Device's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 299 System Time Setting



The following table describes the fields in this screen.

Table 143 System Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.

Table 143 System Time Setting (continued)

LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28 Logs

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs.

28.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

28.1.1 Alerts and Logs

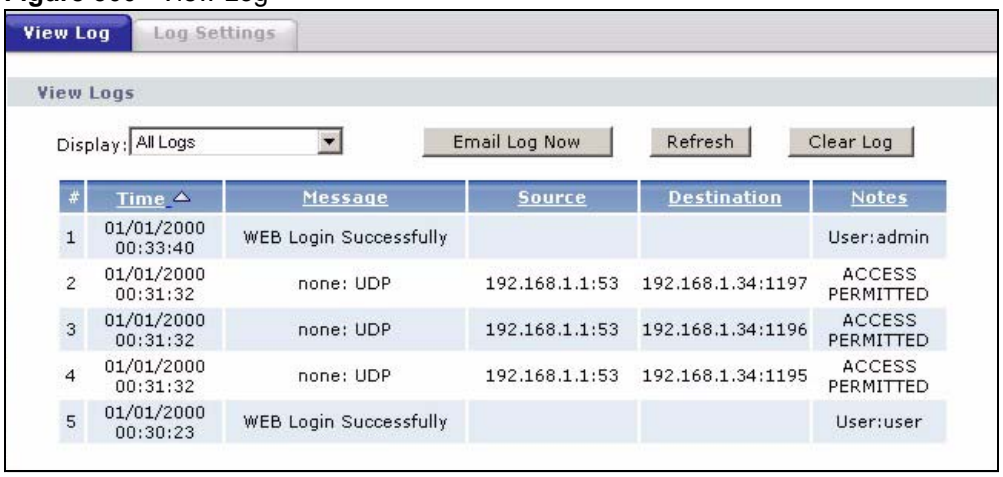
An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

28.2 Viewing the Logs

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 28.3 on page 396).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 300 View Log


View Log
Log Settings
View Logs
Display: All Logs
Email Log Now
Refresh
Clear Log
Time Message Source Destination Notes
1 01/01/2000 00:33:40 WEB Login Successfully User:admin
2 01/01/2000 00:31:32 none: UDP 192.168.1.1:53 192.168.1.34:1197 ACCESS PERMITTED
3 01/01/2000 00:31:32 none: UDP 192.168.1.1:53 192.168.1.34:1196 ACCESS PERMITTED
4 01/01/2000 00:31:32 none: UDP 192.168.1.1:53 192.168.1.34:1195 ACCESS PERMITTED
5 01/01/2000 00:30:23 WEB Login Successfully User:user

The following table describes the fields in this screen.

Table 144 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

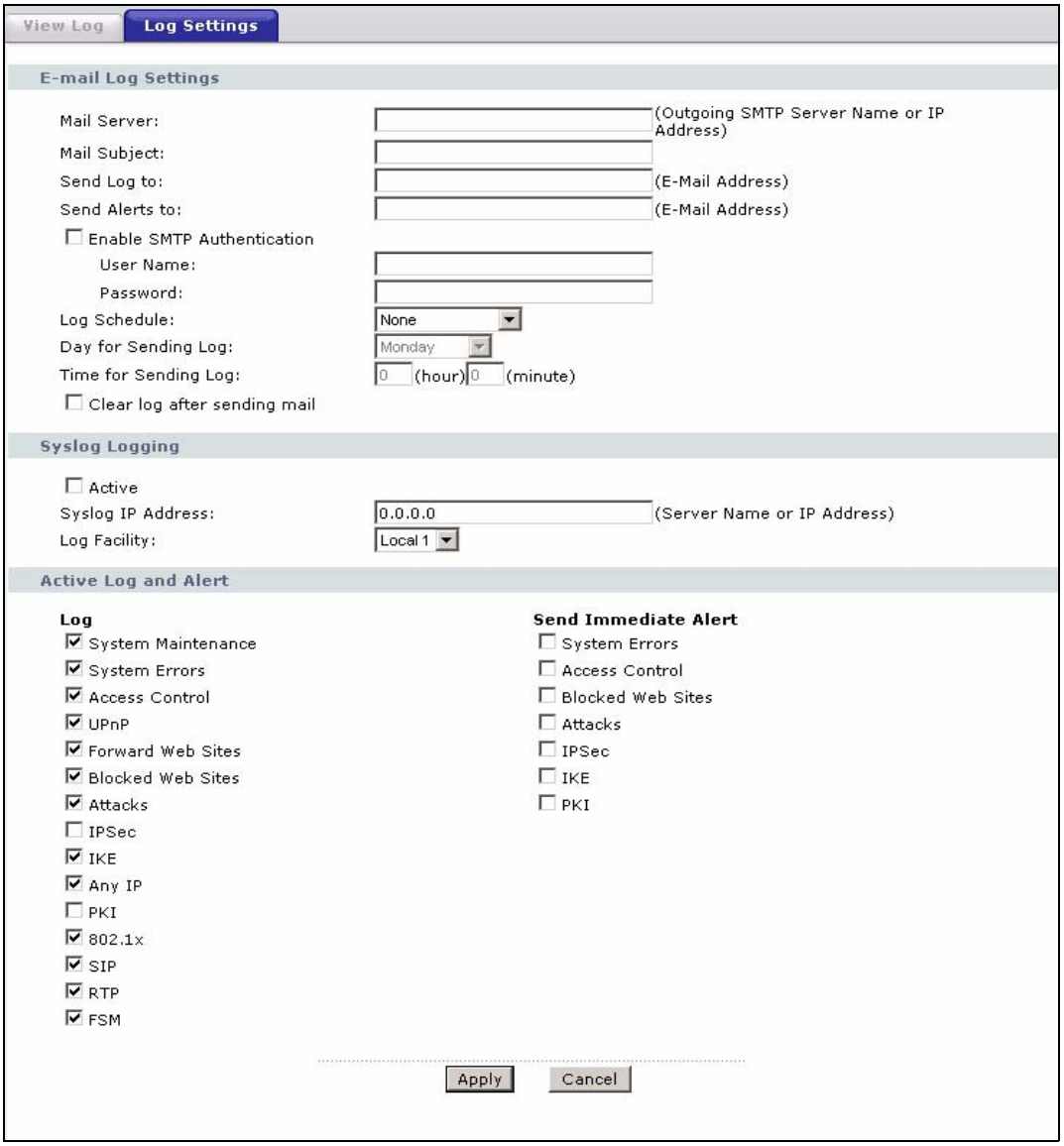
28.3 Configuring Log Settings

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to record. See Section 28.1 on page 395 for more information.

To change your ZyXEL Device's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 301 Log Settings



The following table describes the fields in this screen.

Table 145 Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends. Not all ZyXEL Device models have this field.
Send Log to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.

Table 145 Log Settings

LABEL	DESCRIPTION
Send Alerts to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Enable SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

28.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

“SMTP action request failed. ret= ??". The “??"are described in the following table.

Table 146 SMTP Error Messages

-1 means ZyXEL Device out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

28.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "`End of Log`" message shows that a complete log has been sent.

Figure 302 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

28.5 Log Descriptions

This section provides descriptions of example log messages.

Table 147 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router’s SSH server.
SSH login failed	Someone has failed to log on to the router’s SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 148 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

Table 149 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 150 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600

Table 150 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 151 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 160 on page 405.

Table 152 ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn’t have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

Table 153 CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. “call” is the reference (count) number of the call. “dev” is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or “ch” is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.

Table 153 CDR Logs (continued)

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 154 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 155 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 156 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see Table 160 on page 405.

Table 157 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.

Table 157 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

Table 158 802.1X Logs

LOG MESSAGE	DESCRIPTION
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.

Table 158 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.

Table 159 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/ZyXEL Device)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/ZyXEL Device)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 160 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem

Table 160 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 161 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

Table 162 SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account's registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account's registration from the SIP register server failed.

Table 163 RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

Table 164 FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
VoIP Call Established Ph[Phone Port] -> Outgoing Call Number	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
VoIP Call End Phone[Phone Port]	A VoIP phone call made from a phone connected to the listed phone port has terminated.

Table 165 FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start from SIP[SIP Port Number]	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
VoIP Call Established Ph[Phone Port] <- Outgoing Call Number	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
VoIP Call End Phone[Phone Port]	A VoIP phone call that came into the ZyXEL Device has terminated.

Table 166 PSTN Logs

LOG MESSAGE	DESCRIPTION
PSTN Call Start	A PSTN call has been initiated.
PSTN Call End	A PSTN call has terminated.
PSTN Call Established	A PSTN call has been set up.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to RFC 2408 for detailed information on each type.

Table 167 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature

Table 167 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

29 Tools

This chapter explains how to upload new firmware, manage configuration files and restart your ZyXEL Device.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your ZyXEL Device.

29.1 Introduction

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

29.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. Find this firmware at www.zyxel.com.With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “`config.cfg`”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 168 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

29.3 FTP Restrictions

FTP will not work when:

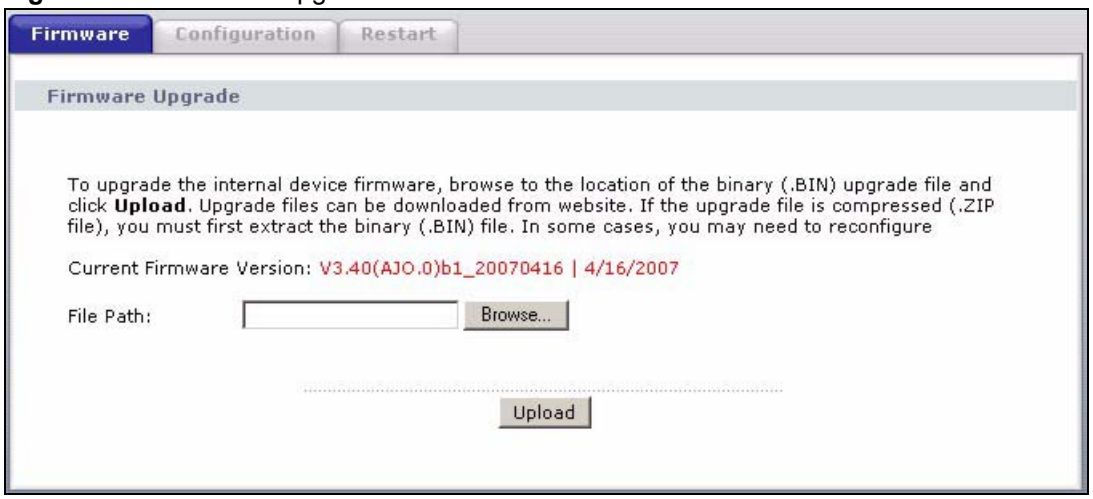
1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
2. You have disabled the FTP service in the **Remote Management** screen.
3. The IP you entered in the **Secured Client IP** field does not match the client IP. If it does not match, the device will disallow the FTP session immediately.

29.4 Firmware Upgrade Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 29.9 on page 418 for upgrading firmware using FTP/TFTP commands.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

Figure 303 Firmware Upgrade


Firmware
Configuration
Restart
Firmware Upgrade
To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure
Current Firmware Version: V3.40(AJO.0)b1_20070416 | 4/16/2007
File Path:
Browse...
Upload

The following table describes the labels in this screen.

Table 169 Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 304 Firmware Upload In Progress

ZyXEL
Firmware Upload In Progress
Do not Turn Off the Device.
Please Wait ...
Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes.
To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 305 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 306 Error Message

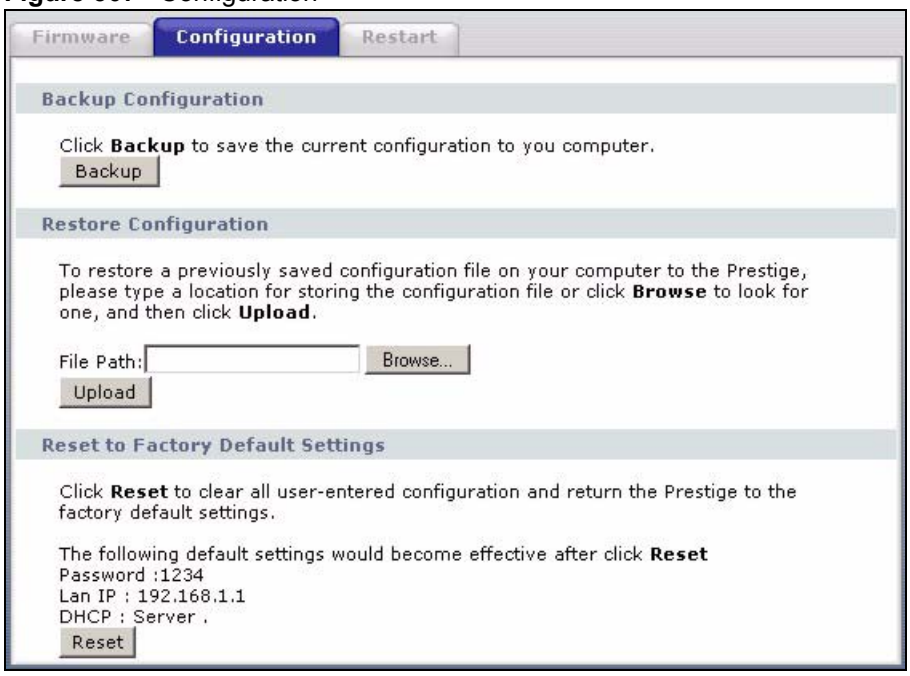
System Upload
Firmware upload error!
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

29.5 Backup and Restore

See Section 29.7 on page 415 and Section 29.8 on page 418 for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 307 Configuration


Firmware
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration to you computer.
Backup
Restore Configuration
To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click Browse to look for one, and then click Upload.
File Path:
Browse...
Upload
Reset to Factory Default Settings
Click Reset to clear all user-entered configuration and return the Prestige to the factory default settings.
The following default settings would become effective after click Reset
Password :1234
Lan IP : 192.168.1.1
DHCP : Server .
Reset

29.5.1 Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

29.5.2 Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Table 170 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 308 Configuration Upload Successful

ZyXEL
Restore Configuration successful
The Router Is Rebooting Now.
Please Wait ...
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 309 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix A on page 1 for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 310 Configuration Upload Error

System Restore
Restore configuration error!
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

29.5.3 Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 311 Reset Warning Message

Microsoft Internet Explorer
Are you sure you want to reset the device back to the factory defaults?This will erase all of your custom configuration.
OK
Cancel

Figure 312 Reset In Process Message

ZyXEL
Reset to Factory Default Settings
Please Wait ...
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to Section 1.6 on page 49 for more information on the **RESET** button.

29.6 Restart

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 313 Restart Screen

Firmware
Configuration
Restart
System Reboot
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

29.7 Using FTP or TFTP to Back Up Configuration

This section covers how to use FTP or TFTP to save your device's configuration file to your computer.

29.7.1 Using the FTP Commands to Back Up Configuration

1 Launch the FTP client on your computer.

2. Enter "open", followed by a space and the IP address of your ZyXEL Device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "bin" to set transfer mode to binary.
6. Use "get" to transfer files from the ZyXEL Device to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyXEL Device to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
7. Enter "quit" to exit the ftp prompt.

29.7.2 FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

Figure 314 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

29.7.3 Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 171 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

29.7.4 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter command "`sys stdio 0`" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command "`sys stdio 5`" to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is "`rom-0`" (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the ZyXEL Device to the computer and "binary" to set binary transfer mode.

29.7.5 TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "`i`" specifies binary image transfer mode (use this mode when transferring binary files), "`host`" is the ZyXEL Device IP address, "`get`" transfers the file source on the ZyXEL Device (`rom-0`, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

29.7.6 Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 172 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyXEL Device and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is "ras" and for the configuration file, is "rom-0".

Table 172 General Commands for GUI-based TFTP Clients (continued)

COMMAND	DESCRIPTION
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to Section 29.3 on page 410 to read about configurations that disallow TFTP and FTP over WAN.

29.8 Using FTP or TFTP to Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.

29.8.1 Restore Using FTP Session Example

Figure 315 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 29.3 on page 410 to read about configurations that disallow TFTP and FTP over WAN.

29.9 FTP and TFTP Firmware and Configuration File Uploads

This section shows you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

29.9.1 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

29.9.2 FTP Session Example of Firmware File Upload

Figure 316 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to Section 29.3 on page 410 to read about configurations that disallow TFTP and FTP over WAN.

29.9.3 TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command "sys stdio 0" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the device to the computer, "put" the other way around, and "binary" to set binary transfer mode.

29.9.4 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the device's IP address, "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

30

Diagnostic

These read-only screens display information to help you identify problems with the ZyXEL Device.

30.1 General Diagnostic

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 317 Diagnostic: General

The following table describes the fields in this screen.

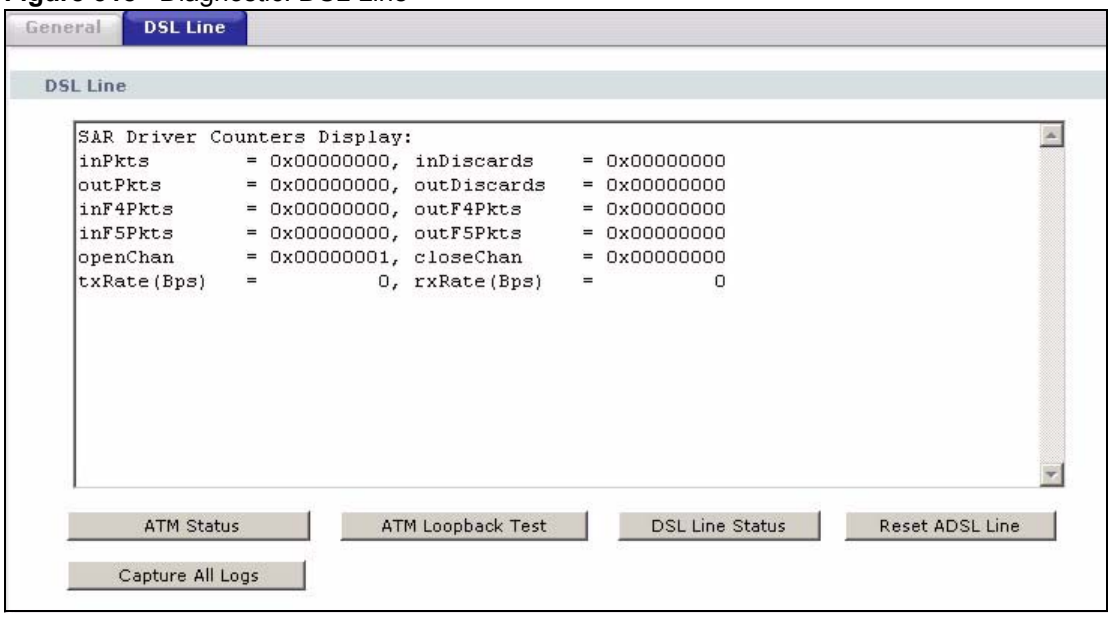
Table 173 Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.

30.2 DSL Line Diagnostic

Click **Maintenance > Diagnostic** > **DSL Line** to open the screen shown next.

Figure 318 Diagnostic: DSL Line



The following table describes the fields in this screen.

Table 174 Diagnostic: DSL Line

LABEL	DESCRIPTION
ATM Status	Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets. These counters are set back to zero whenever the device starts up. **inPkts** is the number of good ATM cells that have been received. **inDiscards** is the number of received ATM cells that were rejected. **outPkts** is the number of ATM cells that have been sent. **outDiscards** is the number of ATM cells sent that were rejected. **inF4Pkts** is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM. **outF4Pkts** is the number of ATM OAM F4 cells that have been sent. **inF5Pkts** is the number of ATM OAM F5 cells that have been received. **outF5Pkts** is the number of ATM OAM F5 cells that have been sent. **openChan** is the number of times that the ZyXEL Device has opened a logical DSL channel. **closeChan** is the number of times that the ZyXEL Device has closed a logical DSL channel. **txRate** is the number of bytes transmitted per second. **rxRate** is the number of bytes received per second.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

Table 174 Diagnostic: DSL Line (continued)

LABEL	DESCRIPTION
DSL Line Status	Click this button to view statistics about the DSL connections. **noise margin downstream** is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is. **output power upstream** is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP. **attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP. Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.

Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:
	`"Start to reset ADSL`
	`Loading ADSL modem F/W...`
	`Reset ADSL Line Successfully!"`

Capture All Logs	Click this button to display information and statistics about your ZyXEL Device's ATM statistics, DSL connection statistics, DHCP settings, firmware version, WAN and gateway IP address, VPI/VCI and LAN IP address.

31

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access
- Phone Calls and VoIP
- Multiple SIP Accounts
- USB Device Connection

31.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 48.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

31.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1. The default IP address is **192.168.1.1**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 49.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 49.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section 9.3.1 on page 144), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 453.
4. If you disabled **Any IP** (Section 9.4.1 on page 148), make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix A on page 1. Your ZyXEL Device is a DHCP server by default.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See Appendix A on page 1.

5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.6 on page 49.
6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the WAN port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the user name and password correctly. The default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
3 Turn the ZyXEL Device off and on.
4 If this does not work, you have to reset the device to its factory defaults. See Section 31.1 on page 425.

I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

31.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 48.
2. Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 48.
2. Turn the ZyXEL Device off and on.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 48. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Turn the ZyXEL Device off and on.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

31.4 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1. Check the telephone connections and telephone wire.
2. Make sure you have the **VoIP SIP Settings** screen properly configured.

I can access the Internet, but cannot make VoIP calls.

1. Make sure you have the **VoIP SIP Settings** screen properly configured.
2. The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
3. You can also check the VoIP status in the **Status** screen.
4. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

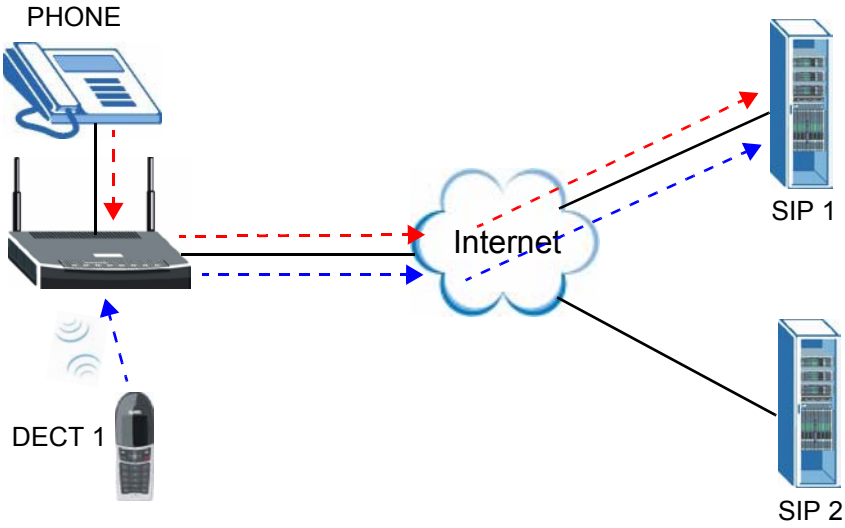
31.5 Multiple SIP Accounts

You can set up two SIP accounts on your ZyXEL Device and your ZyXEL Device is equipped with two phone ports. By default your ZyXEL Device uses SIP account 1 with all connected phones for outgoing calls, and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone ports in order to control which SIP account you are using when placing or receiving calls.

31.5.1 Outgoing Calls

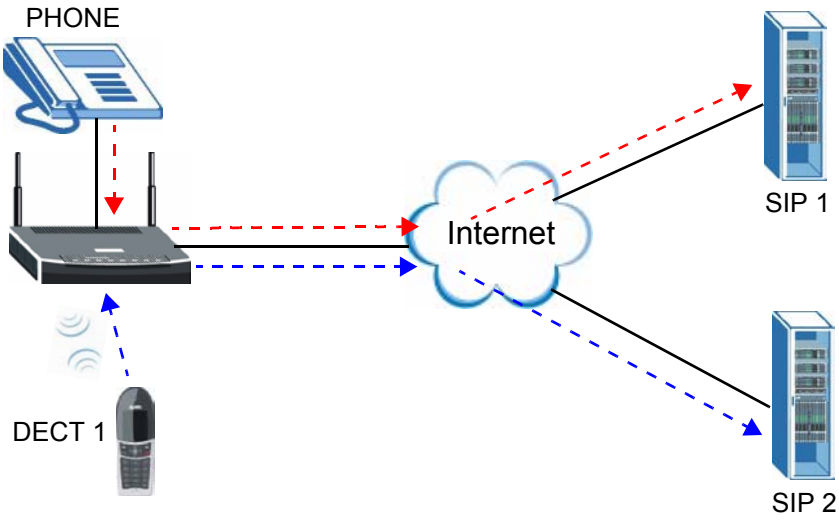
The following figure represents the default behavior of your ZyXEL Device when two SIP accounts are configured and you are using two phones. When you place a call from the **PHONE** port or DECT phone 1, the ZyXEL Device will use SIP account 1.

Figure 319 Outgoing Calls: Default



In the next example, the **PHONE** port is configured to use SIP account 1 and DECT phone 1 is configured to use SIP account 2. In this case, every time you place a call through the **PHONE** port, you are using your SIP account 1. Similarly, every time you place a call through DECT phone 1, you are using your SIP account 2. To apply these configuration changes you need to configure the **Analog Phone** and **DECT Phone** screens. See Section 12.8 on page 200.

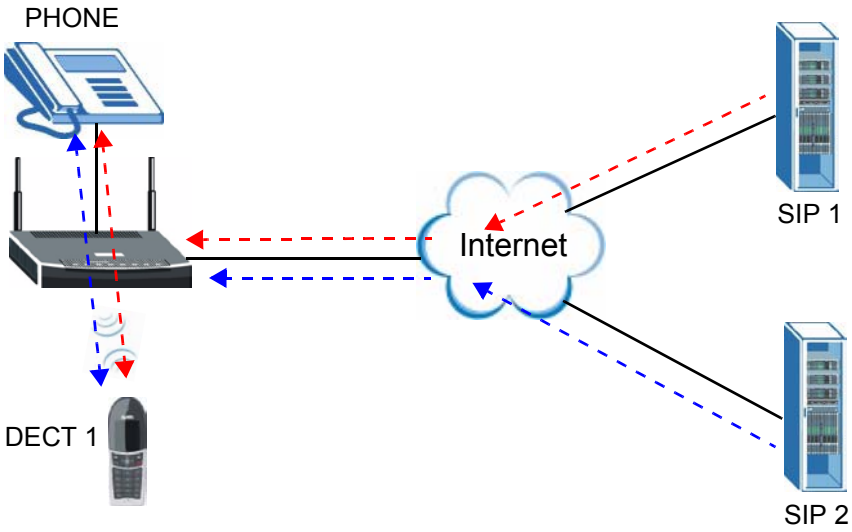
Figure 320 Outgoing Calls: Individual Configuration



31.5.2 Incoming Calls

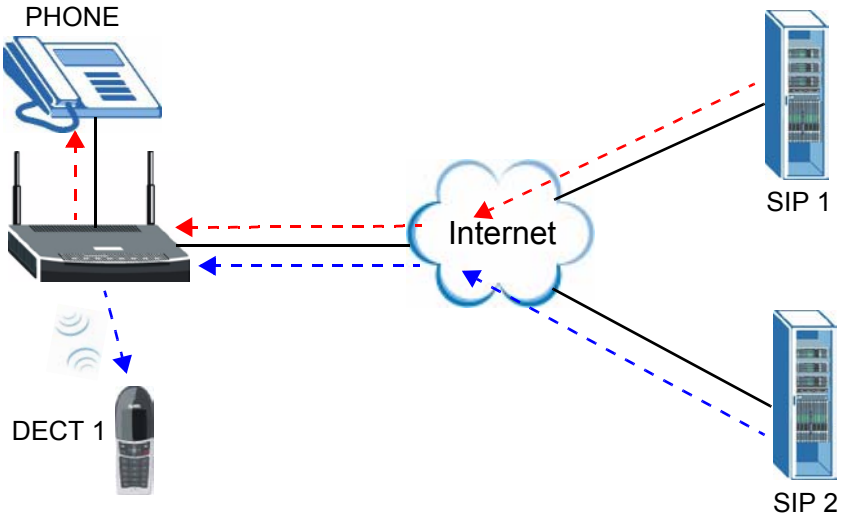
The following example shows the default behavior of your ZyXEL Device for incoming calls when two SIP accounts are configured and you are using two phones. When a call comes in from your SIP account 1, both the phone connected to the **PHONE** port and DECT phone 1 ring. Similarly, when a call comes in from your SIP account 2, both the phone connected to the **PHONE** port and DECT phone 1 ring. In either case you are not sure which SIP account the call is coming from.

Figure 321 Incoming Calls: Default



In the next example, the **PHONE** port is configured to use SIP account 1 and DECT phone 1 is configured to use SIP account 2 for incoming calls. In this case, every time you receive a call from your SIP account 1, the phone connected to the **PHONE** port rings. Similarly, every time you receive a call from your SIP account 2, DECT phone 1 rings. To apply these configuration changes you need to configure the **Analog Phone** and **DECT Phone** screens. See Section 12.8 on page 200.

Figure 322 Incoming Calls: Individual Configuration



31.6 USB Device Connection

The ZyXEL Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the ZyXEL Device.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Re-connect your USB device to the ZyXEL Device.

32

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Hardware Specifications

Table 175 Hardware Specifications

Dimensions	(168 W) x (37 D) x (248 H) mm
Weight	390g
Power Specification	18VAC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
PHONE Ports	1 RJ-11 FXS POTS port
PSTN Line port	1 RJ-11 FXS POTS port for making calls over the PSTN line.
RESET Button	Restores factory defaults
Antenna	One attached external dipole antenna, 2dBi
Operation Temperature	0º C ~ 40º C
Storage Temperature	-30º ~ 60º C
Operation Humidity	10% ~ 85% RH
Storage Humidity	10% ~ 90% RH

Firmware Specifications

Table 176 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Server IP Pool	192.168.1.32 to 192.168.1.64
Static DHCP Addresses	10
The number of DECT phones your ZyXEL Device supports	6

Table 176 Firmware Specifications (continued)

The range of your ZyXEL Device during the registration process	Outdoor : 300 Meters Indoor : 50 Meters
Content Filtering	Web page blocking by URL keyword.
Static Routes	16 IP
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The ZyXEL Device blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering. You can also subscribe to category-based content filtering that allows your ZyXEL Device to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.

Table 176 Firmware Specifications (continued)

Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.
Zero Configuration Internet Access	Once you connect and turn on the device, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.
Any IP	The Any IP feature allows a computer to access the Internet and the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
IPSec VPN Capability	Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyXEL Device VPN is based on the IPSec standard and is interoperable with other IPSec-based VPN products. The ZyXEL Device supports up to two simultaneous IPSec connections.
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
Content Filtering	Content filtering allows you to block access to Internet web sites that contain key words (that you specify) in the URL. You can also schedule when to perform the filtering and give trusted LAN IP addresses unfiltered Internet access.
Media Bandwidth Management	Media Bandwidth Management allows you to specify bandwidth classes based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Dynamic DNS Support	With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

Table 176 Firmware Specifications (continued)

DHCP	DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Packet Filters	Your device's packet filtering function allows added network security and management.
ADSL Standards	Support ITU G.992.1 G.dmt (Annex B, U-R2) EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL 2/2+ AnnexM ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) Multiple PPPoE VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM Zero configuration
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator CLI (Command Line Interpreter) SNMP v1 & v2c with MIB II Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore Telnet for remote management Remote Management Control: Telnet, FTP, Web, SNMP and DNS. VoIP Auto-provisioning via TFTP / HTTP / HTTPS Remote Firmware Upgrade Syslog

Table 176 Firmware Specifications (continued)

Other Features	Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS SPTGEN QoS
Firewall	Stateful Packet Inspection Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc. Access Control of Service Content Filtering IP & Generic Packet Filtering Real time Attack Alerts and Logs Reports and logs SIP ALG passthrough
NAT/SUA	Port Forwarding 2048 NAT sessions Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough
VPN	2 IPSec tunnels IKE and Manual Key Management AH and ESP Protocol DES, 3DES and AES Encryption SHA-1 and MD5 Authentication Tunnel and Transport Mode Encapsulation IPSec NAT Traversal NETBIOS pass-through for IPSec

Voice Specifications

To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

Not all features are supported by all service providers. Consult your service provider for more information.

Table 177 Voice Features

Call Fallback	Call fallback allows you to set the ZyXEL Device to automatically use the PSTN connection for outgoing calls if the SIP account is not working, or to use the SIP account for outgoing calls if the PSTN port is unplugged or not working.
Call Park and Pickup	Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). You can continue the call on the same phone, or another phone connected to the ZyXEL Device. The caller must still pay while the call is parked. When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call. You can have more than one call on hold at the same time, but you must give each call a different number.
Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.
Country Code	Phone standards and settings differ from one country to another, so the settings on your ZyXEL Device must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the ZyXEL Device from one country to another.
Distinctive Ringing	With the distinctive ring feature, you can assign different ringing tones to different incoming calls, based either on the number that calls you or from where the call originates (SIP, PSTN or internal). Use this feature to let you know where a call comes from before you answer it.
Do not Disturb (DnD)	This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter.
Auto Dial	You can set the ZyXEL Device to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the ZyXEL Device wait a specified length of time before dialing the number.
Music on hold	This feature allows you to put a call on hold and have the other person hear a piece of audio (music, speech, etc.) you previously recorded.
Phone config	The phone config table allows you to customize the phone keypad combinations you use to access certain features on the ZyXEL Device, such as call waiting, call return, call forward, etc. The phone config table is configurable in command interpreter mode.
Internal call	When you have phones attached to both of the ZyXEL Device's phone ports, you can dial "####" to place a call to the phone(s) connected to the other port.
HTTP pincode	If your service provider uses an auto provisioning server, you need to enter a personal identification number (supplied by your service provider) before you first use the feature.
Firmware update enable / disable	If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your ZyXEL Device. Enter *99# in your phone's keypad to have the ZyXEL Device upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.

Table 177 Voice Features

Call forwarding	With this feature, you can set the ZyXEL Device to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The ZyXEL Device supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
Trunking	Trunking connects an IP network (like the Internet) with the regular telephone network (PSTN). The main advantage of trunking is that you can call your ZyXEL Device on the PSTN network, and then use it to make a VoIP phonecall. For example, if you have a ZyXEL Device at your office you can call into it from your cellphone and use it to make a long-distance or international VoIP call at a reduced cost.
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Multiple SIP Accounts	You can simultaneously use multiple voice (SIP) accounts and assign them to one or both telephone ports.
Multiple Voice Channels	Your device can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.
Voice Activity Detection/Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	You device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Other Voice Features	SIP version 2 (Session Initiating Protocol RFC 3261) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711, G.726, G.729 Fax and data modem discrimination DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Point-to-point call establishment between two IADs Quick dialing through predefined phone book, which maps the phone dialing number and destination URL. Flexible Dial Plan (RFC3525 section 7.1.14)

Wireless Features

Table 178 Wireless Features

IEEE 802.11g+ Wireless LAN	Your device supports IEEE 802.11g+ to allow any ZyXEL WLAN devices that also support IEEE 802.1g+ to associate with the ZyXEL Device at higher transmission speeds than with standard IEEE 802.11g.
External Antenna	The ZyXEL Device is equipped with an attached antenna to provide a clear radio signal between the wireless stations and the access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.
Other Wireless Features	IEEE 802.11g Compliance Frequency Range: 2.4 GHz ISM Band Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps, and 1 Mbps Auto Fallback Turn on-off WLAN by reset button (press 1s on reset button to turn on or turn off the WLAN; 5s for OTIST; 10s to reset back to factory default) WPA2 WMM IEEE 802.11i IEEE 802.11e Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit. WLAN bridge to LAN Up to 32 MAC Address filters IEEE 802.1x Store up to 32 built-in user profiles using EAP-MD5 (Local User Database) External RADIUS server using EAP-MD5, TLS, TTLS OTIST (ZyXEL's One-Touch Intelligent Security Technology)

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 179 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Your device may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 180 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol

Table 180 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g+	Turbo and Super G modes
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
MBM v2	Media Bandwidth Management v2
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management.
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

Power Adaptor Specifications

Table 181 P-2602HWL Series Power Adaptor Specifications

North American PLUG standards	OEM (Original Equipment Manufacturer)	LEI (LEADER ELECTRONICS INC.)
AC Power Adapter Model	ADS18B-W 180100	MU18-2180100-A1
Input Power	AC 100~240Volts/50/60Hz/0.5A	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	UL,CUL(UL 60950-1)	UL,CUL(UL 60950-1)
EUROPEAN PLUG STANDARDS		
AC Power Adapter Model	ADS18B-B 180100	MU18-2180100-C5
Input Power	AC 100~240Volts/50/60Hz/0.5A	AC 100~240Volts/50/60Hz/0.6A

Table 181 P-2602HWL Series Power Adaptor Specifications (continued)

Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	TUV, CE(EN 60950 -1)	TUV, CE(EN 60950-1)
UNITED KINGDOM PLUG STANDARDS		
AC Power Adapter Model	ADS18B-D 180100	MU18-2180100-B2
Input Power	AC 100~240Volts/50/60Hz/0.5A	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	TUV, CE(EN 60950 -1)	TUV, CE(EN 60950-1)

PART V Appendices and Index

The appendices provide general information. Some details may not apply to your ZyXEL Device.

Setting up Your Computer's IP Address (447)

Pop-up Windows, JavaScripts and Java Permissions (453)

IP Addresses and Subnetting (477)

Wireless LANs (467)

Services (499)

Command Interpreter (481)

Internal SPTGEN (503)

Legal Information (527)

Customer Support (531)

Index (537)

A

Setting up Your Computer's IP Address

The purpose of this appendix is to show you how to configure an IP address on your computer depending on what operating system you have. It does NOT mean that your ZyXEL Device supports all these operating systems.

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

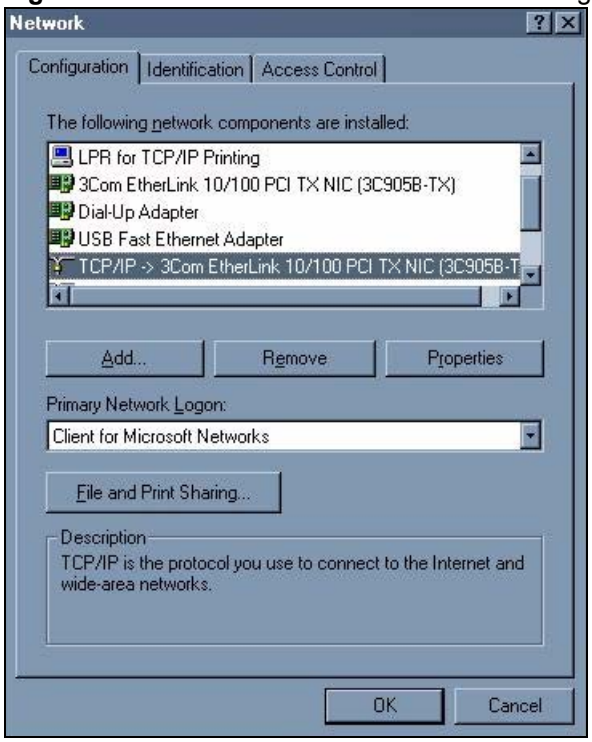
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 323 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

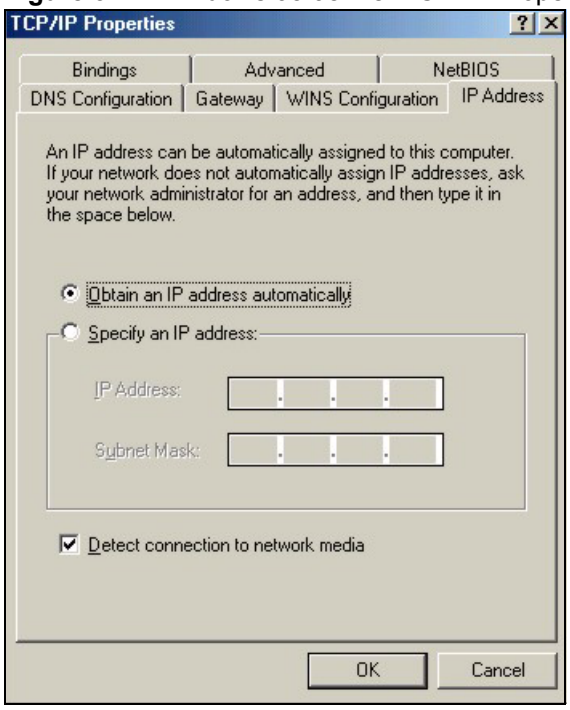
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

Configuring

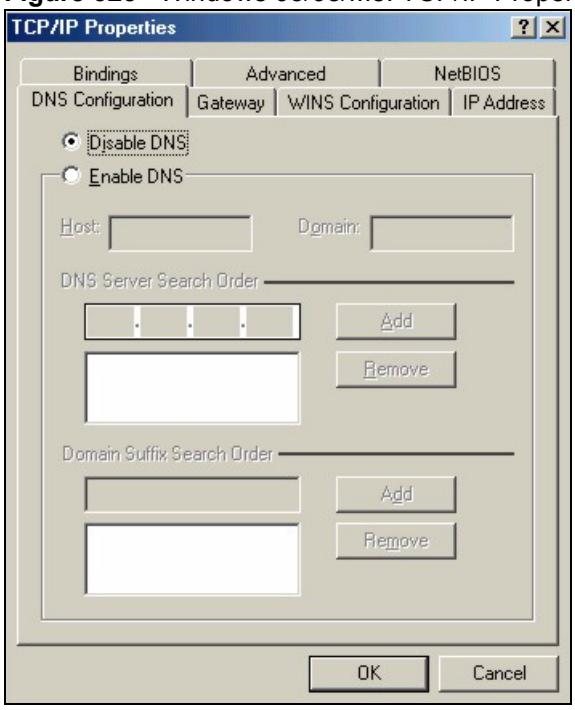
1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 324 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3. Click the **DNS** Configuration tab.
   - If you do not know your DNS information, select **Disable DNS**.
   - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 325 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

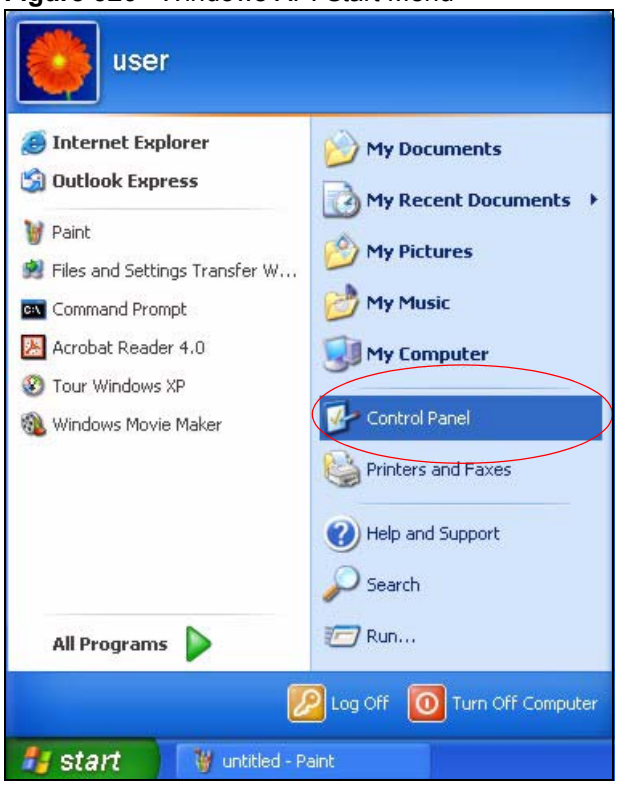
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 326 Windows XP: Start Menu

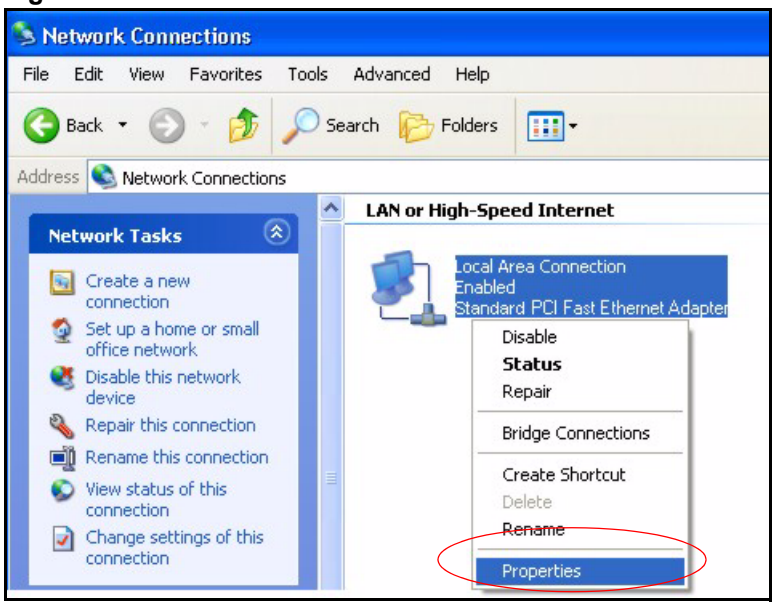


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 327 Windows XP: Control Panel

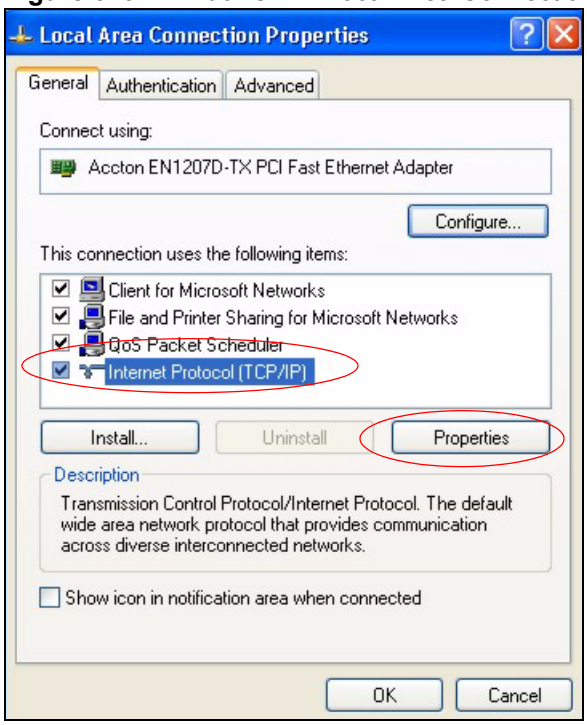
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 328 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

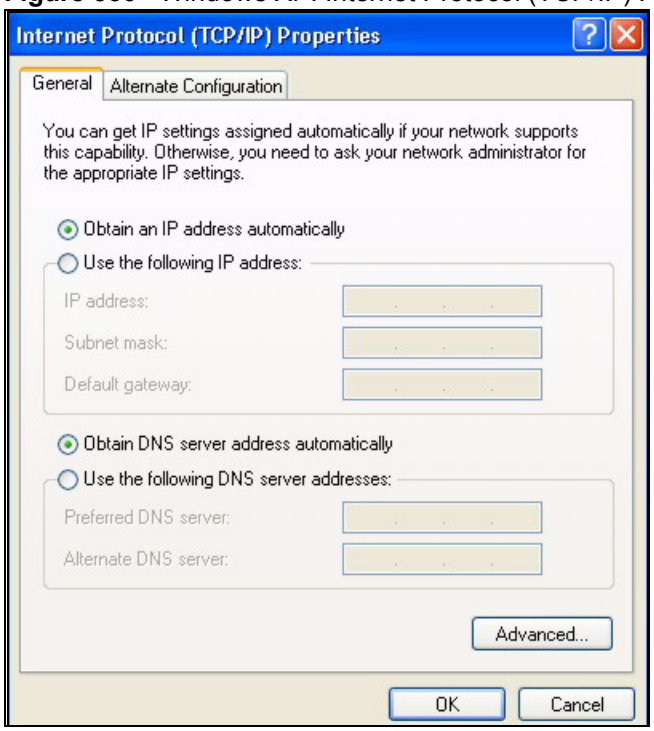
Figure 329 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 330 Windows XP: Internet Protocol (TCP/IP) Properties

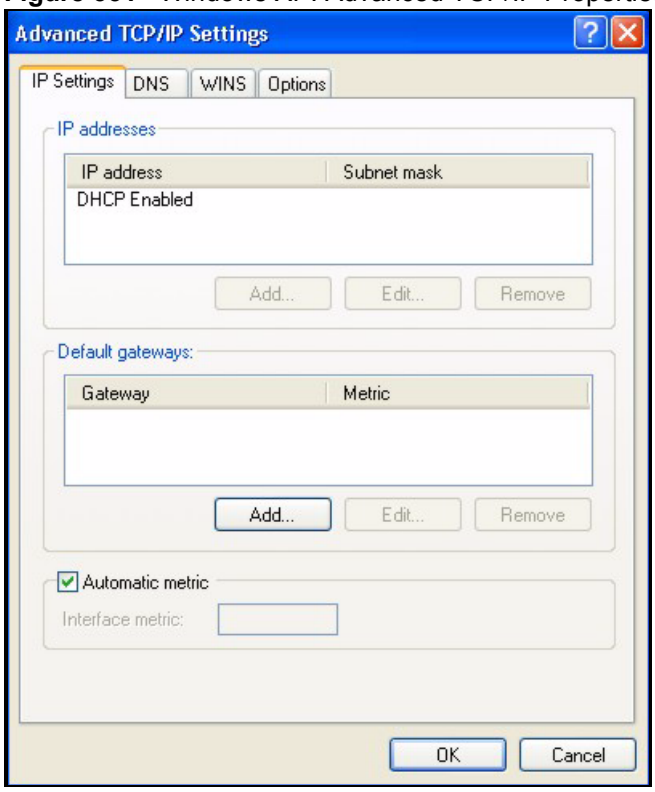

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 331 Windows XP: Advanced TCP/IP Properties

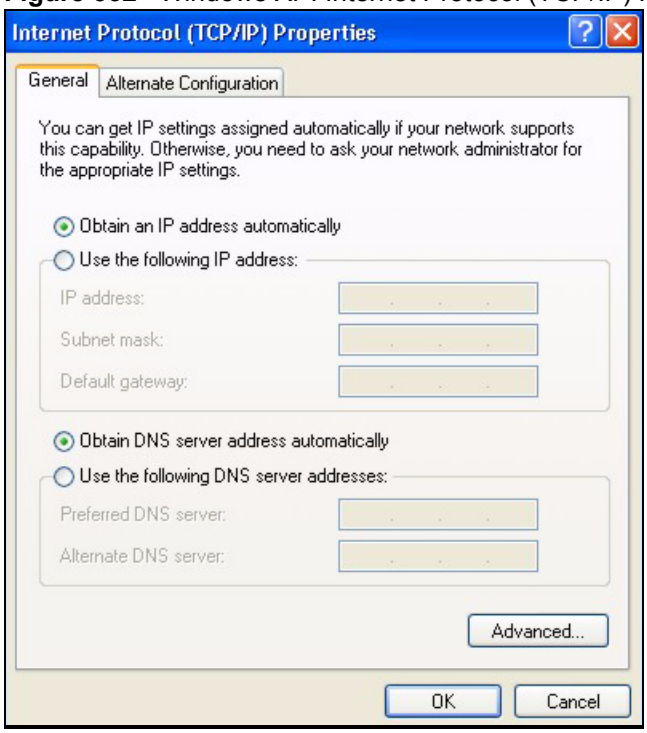


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 332 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

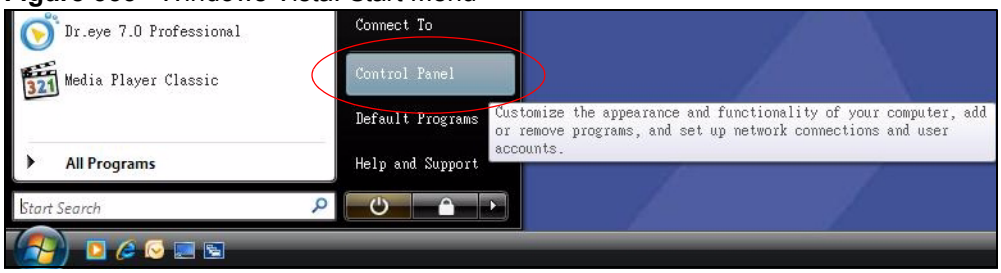
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

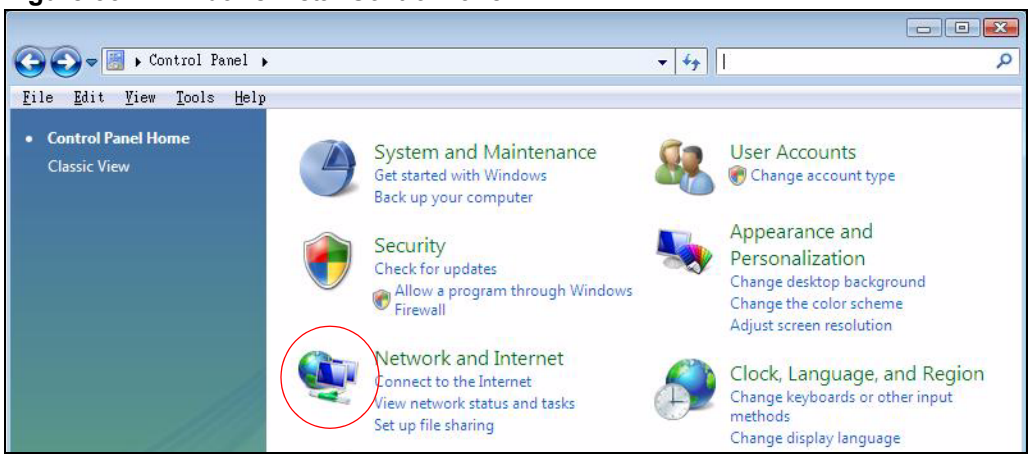
1 Click the **Start** icon, **Control Panel**.

Figure 333 Windows Vista: Start Menu


Dr.eye 7.0 Professional
Media Player Classic
All Programs
Start Search
Connect To
Control Panel
Default Programs
Help and Support
Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

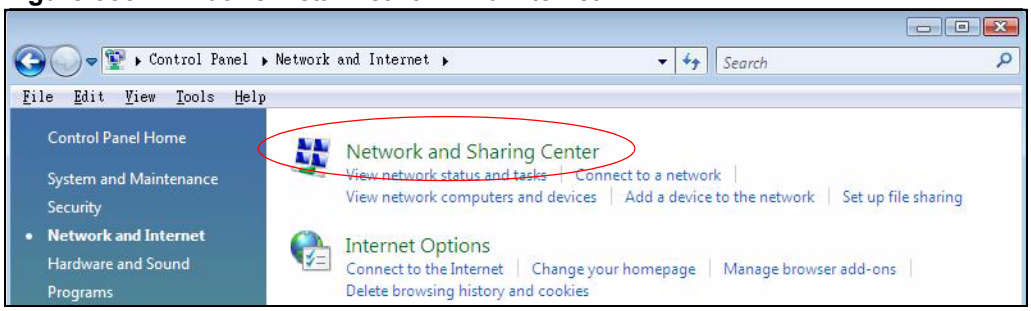
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 334 Windows Vista: Control Panel



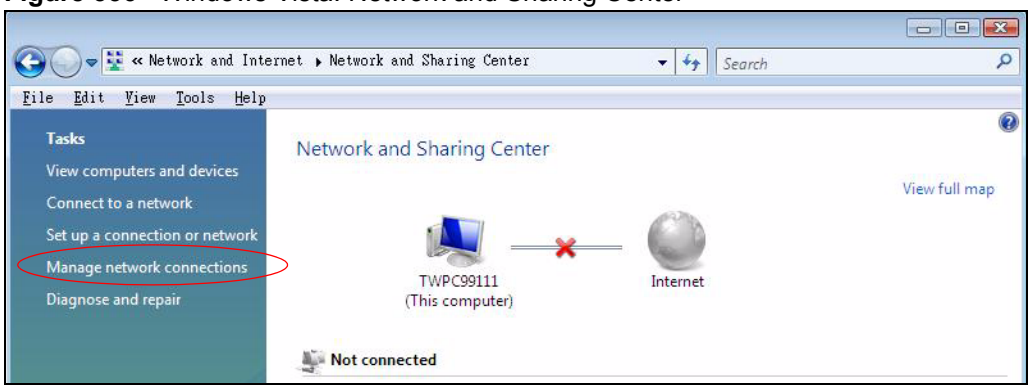
3 Click **Network and Sharing Center**.

Figure 335 Windows Vista: Network And Internet



4 Click **Manage network connections**.

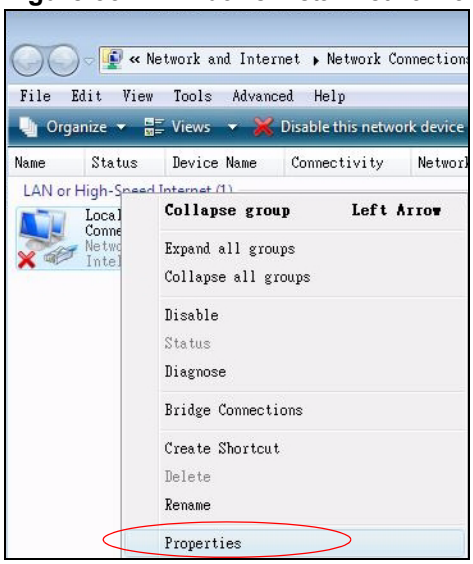
Figure 336 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then click **Properties**.

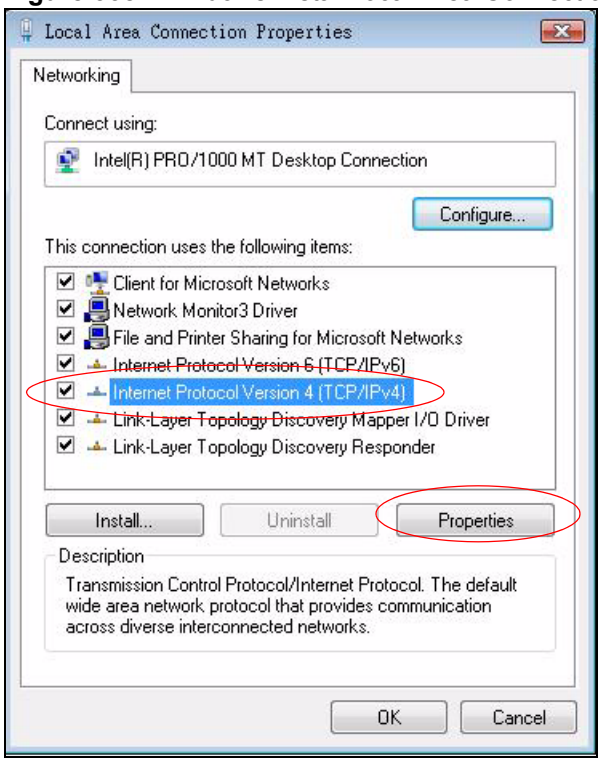
During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 337 Windows Vista: Network and Sharing Center



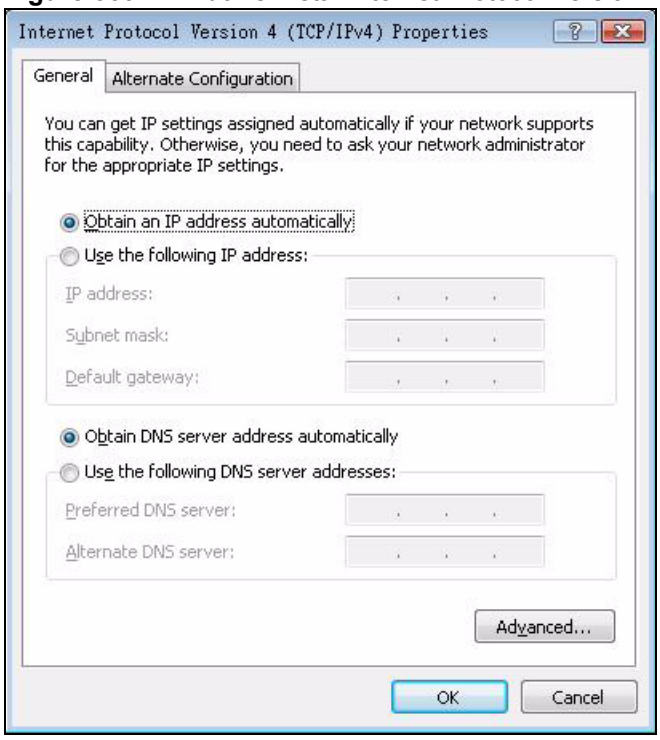
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 338 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).
- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 339 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

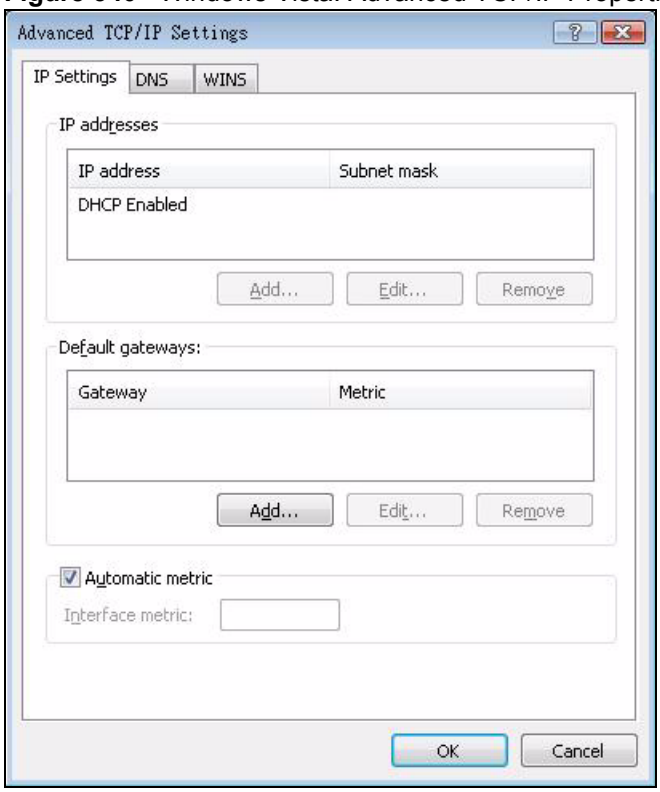

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 340 Windows Vista: Advanced TCP/IP Properties

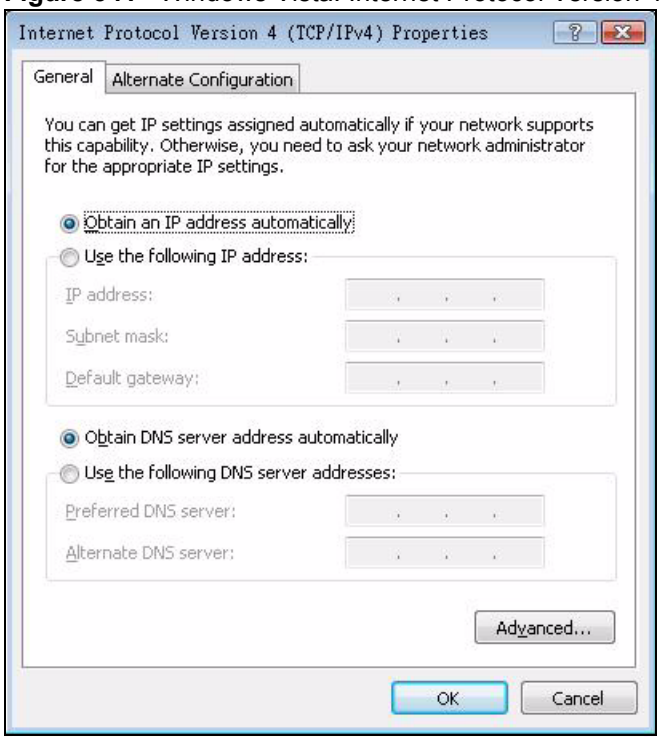


9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 341 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

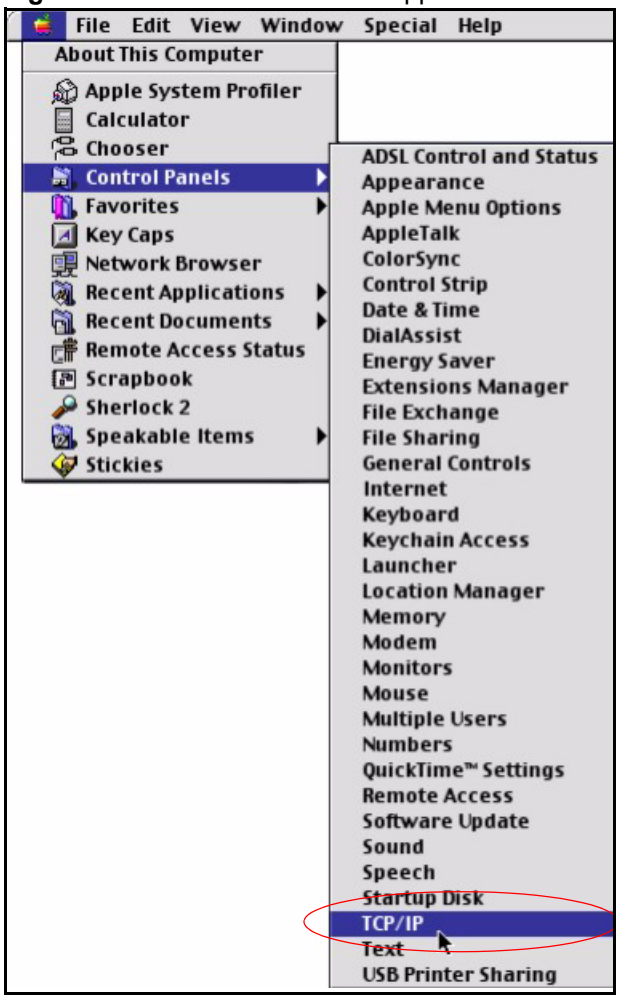
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

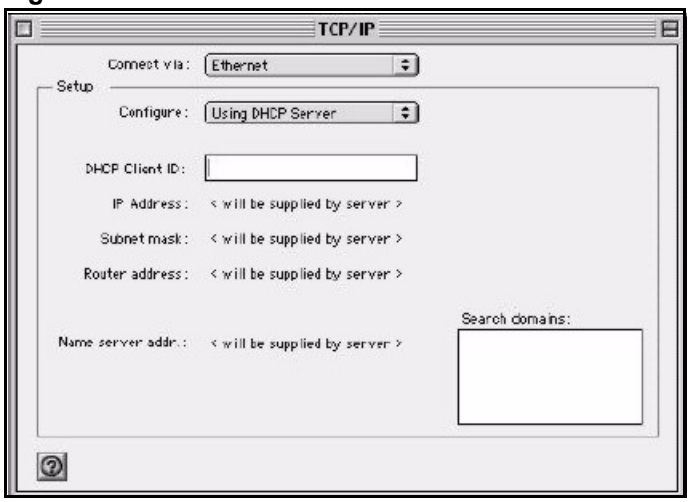
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 342 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 343 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

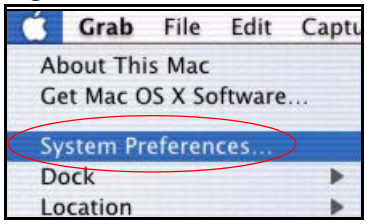
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 344 Macintosh OS X: Apple Menu

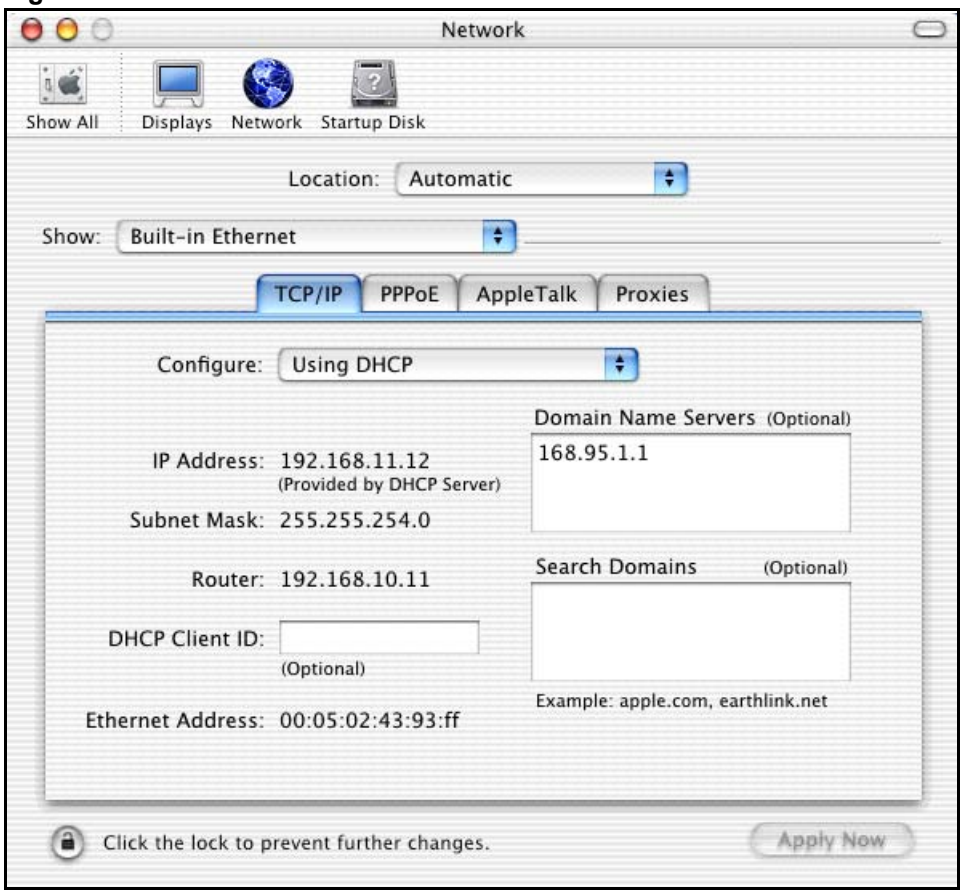


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 345 Macintosh OS X: Network



4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your ZyXEL Device in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

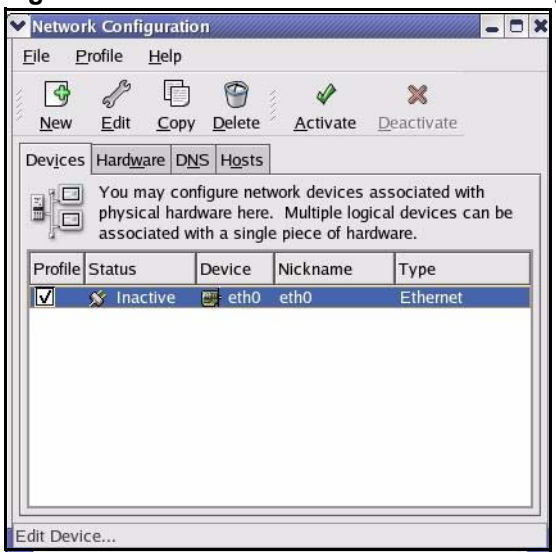
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 346 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

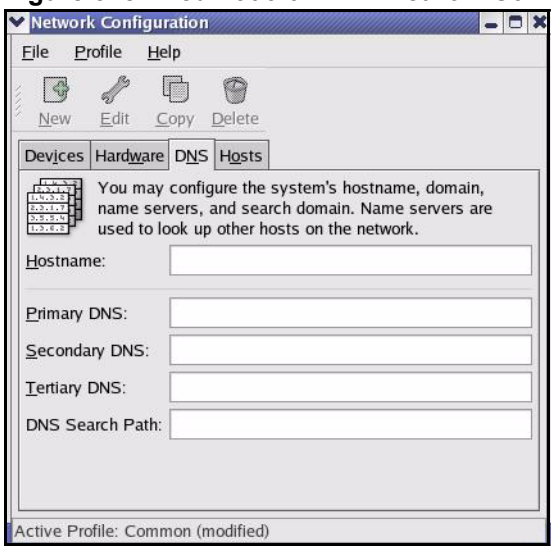
Figure 347 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 348 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 349 Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 350 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 351 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 352 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 353 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 354 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

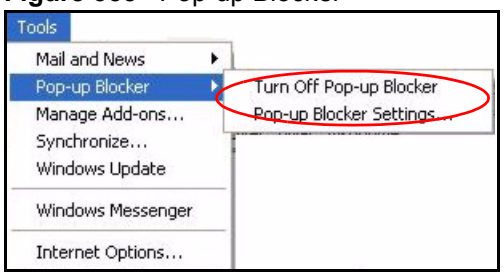
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 355 Pop-up Blocker

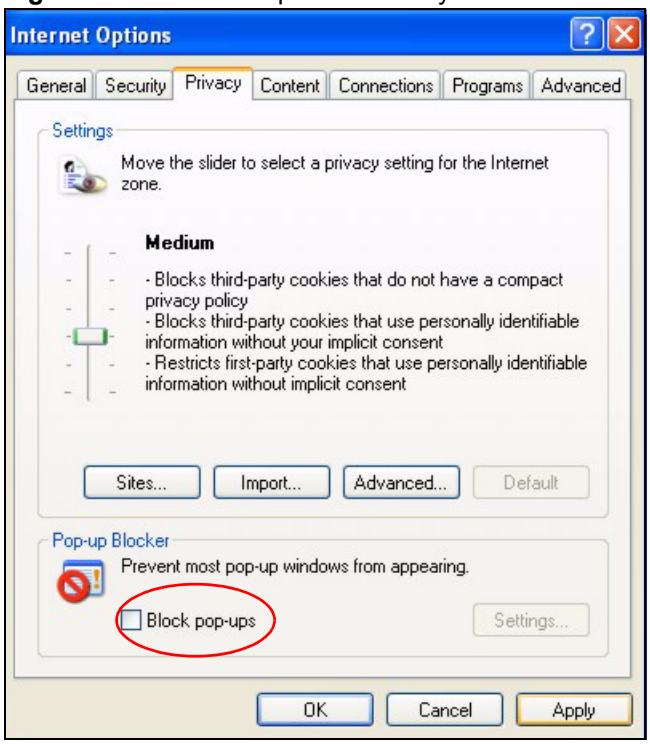


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 356 Internet Options: Privacy



3 Click **Apply** to save this setting.

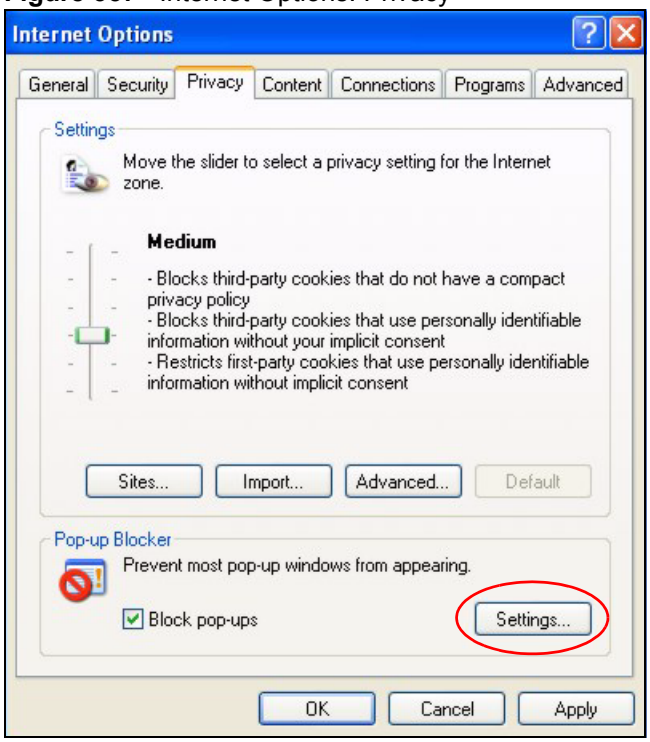
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

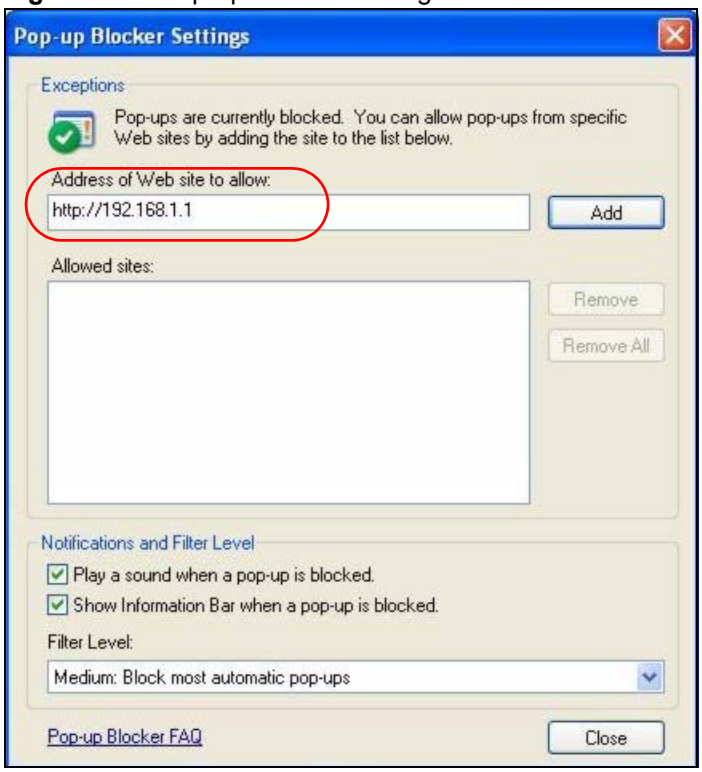
Figure 357 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 358 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

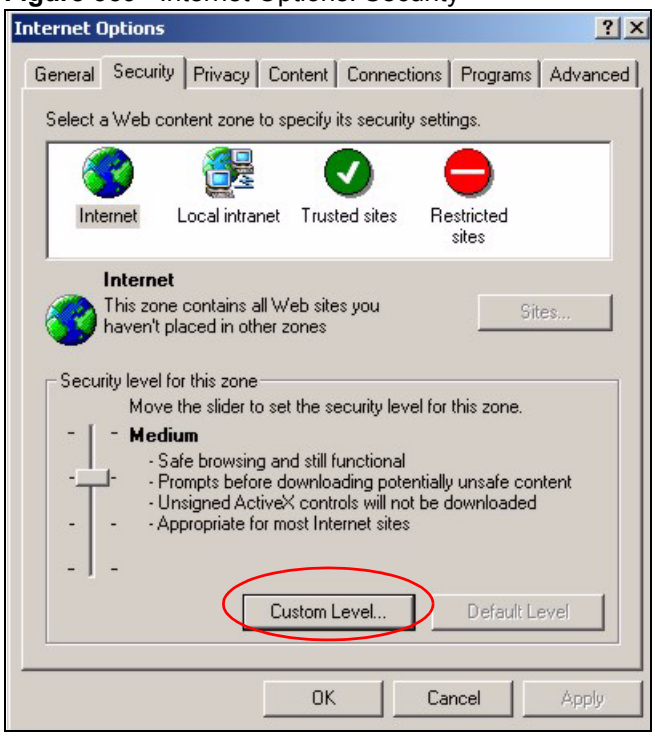
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

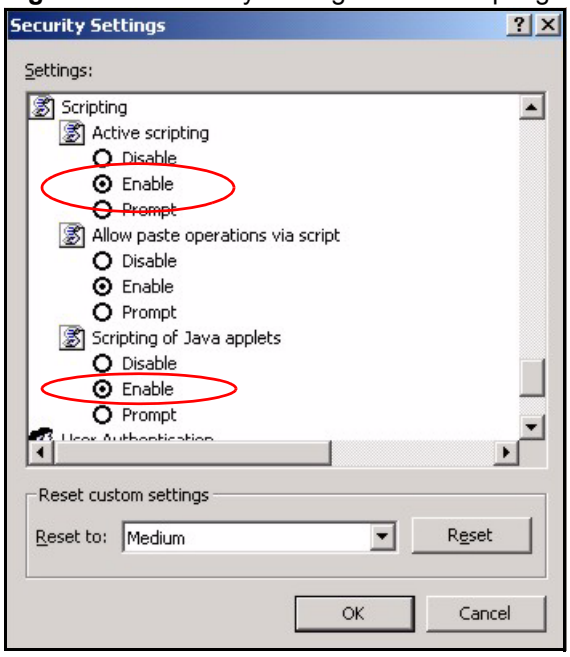
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 359 Internet Options: Security



2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

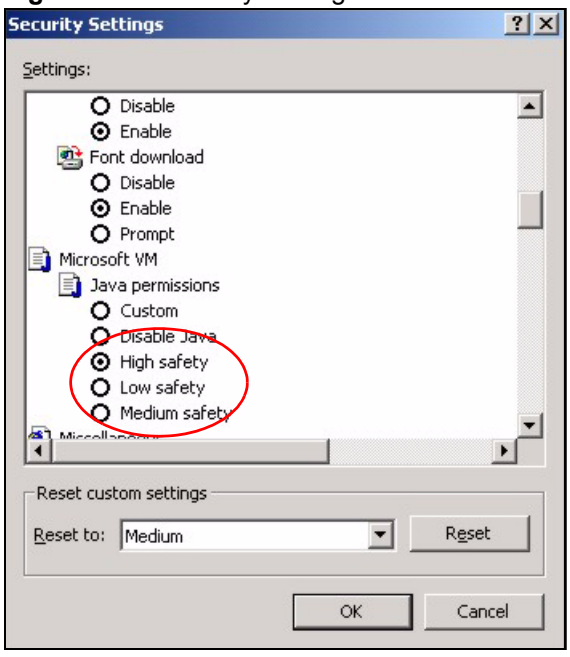
Figure 360 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

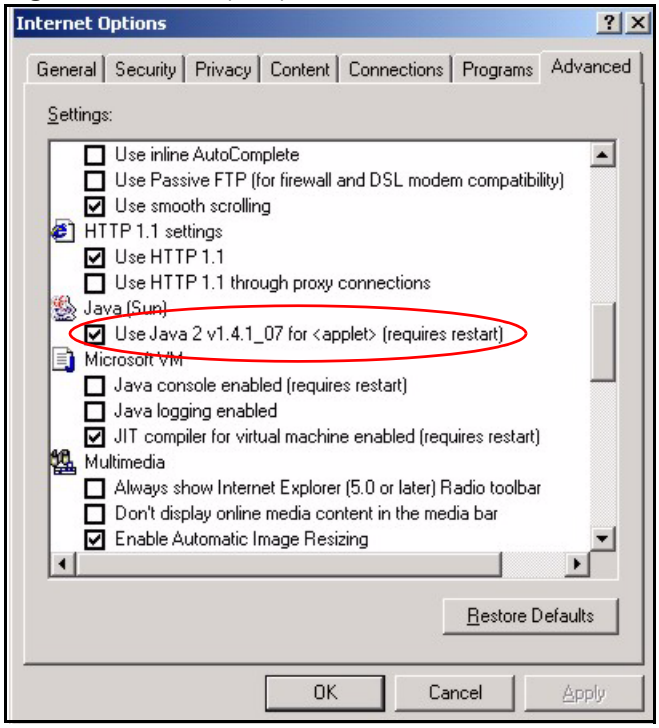
Figure 361 Security Settings - Java



JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3 Click **OK** to close the window.

Figure 362 Java (Sun)

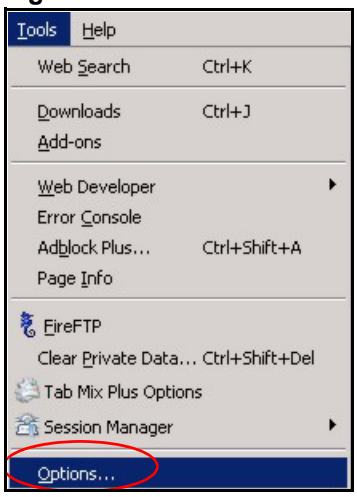


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

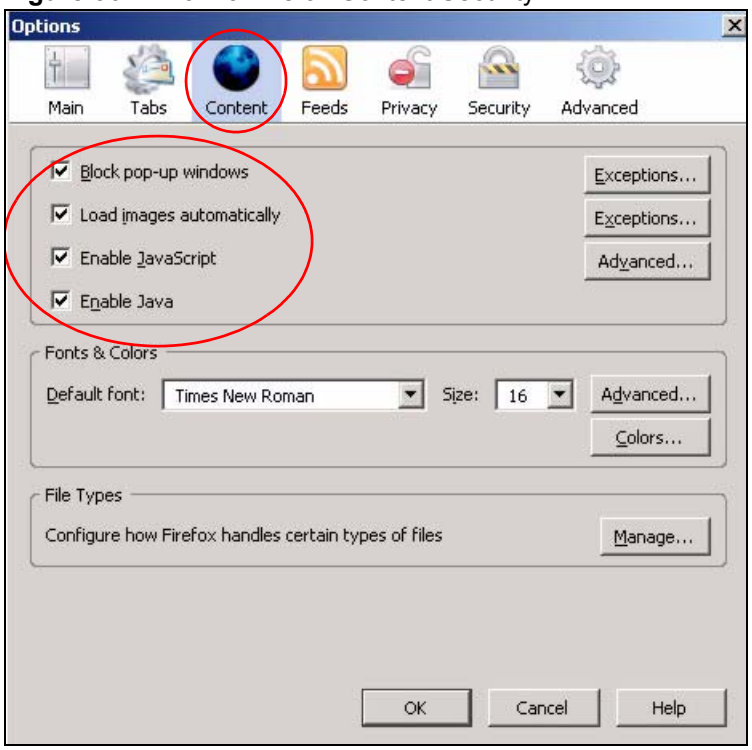
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 363 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 364 Mozilla Firefox Content Security



C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

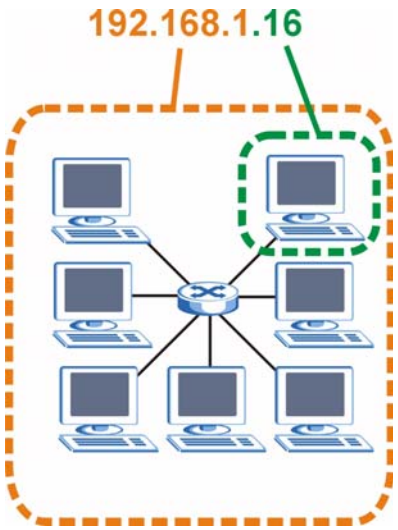
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 365 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 182 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 183 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 184 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 185 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 185 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

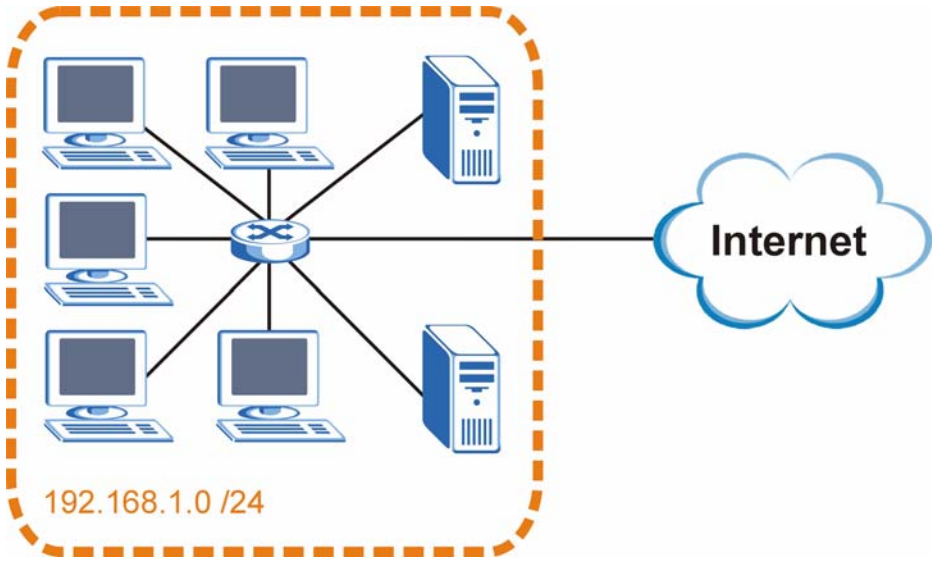
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 366 Subnetting Example: Before Subnetting

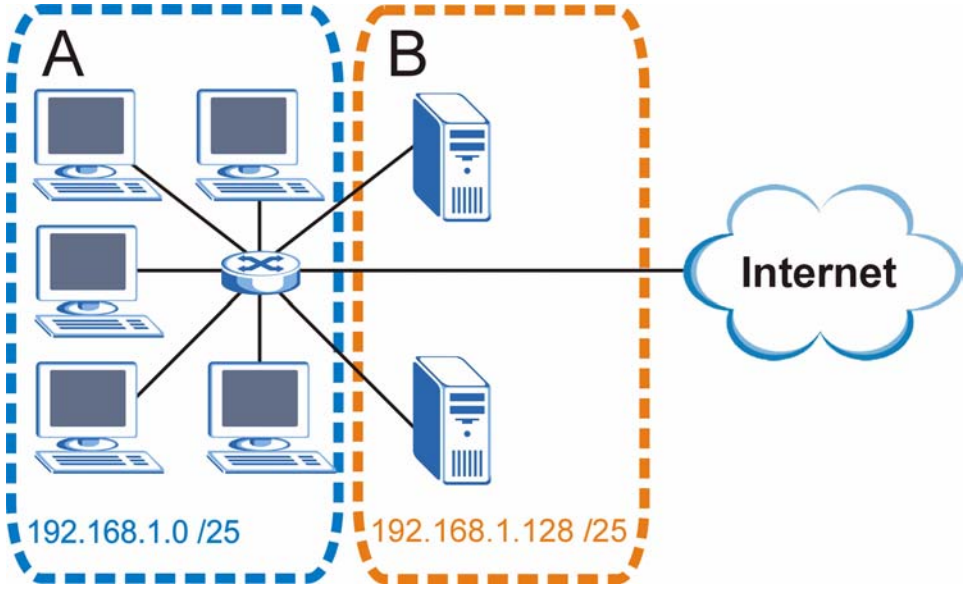


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 367 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 186 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 187 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 188 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 189 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 190 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 190 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 191 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 192 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 192 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

D

Wireless LANs

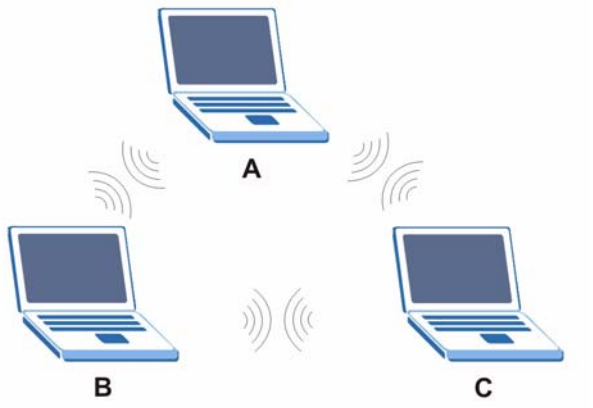
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 368 Peer-to-Peer Communication in an Ad-hoc Network

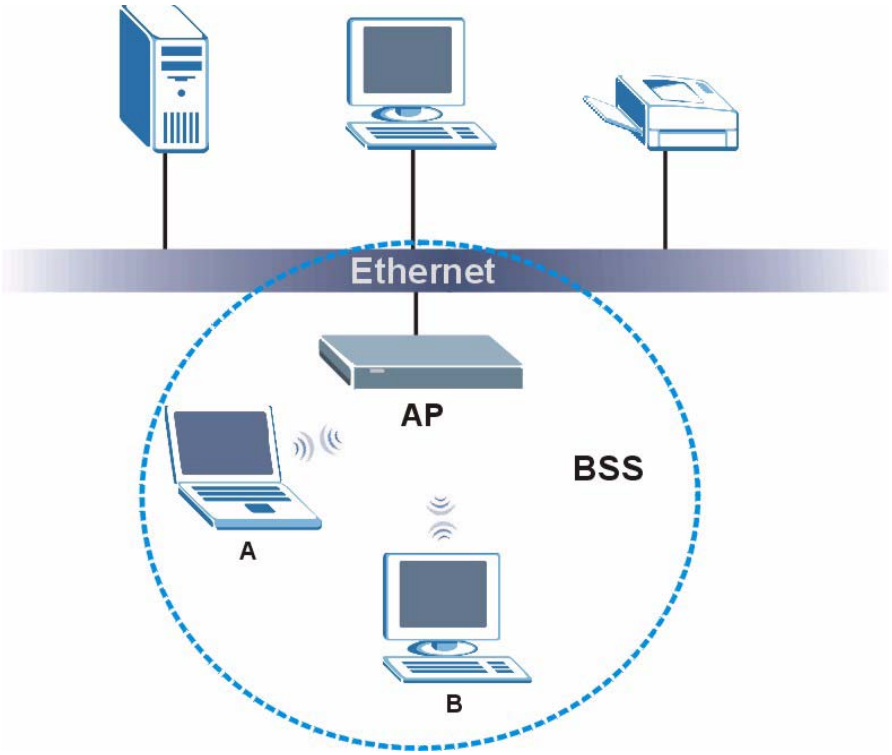


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 369 Basic Service Set



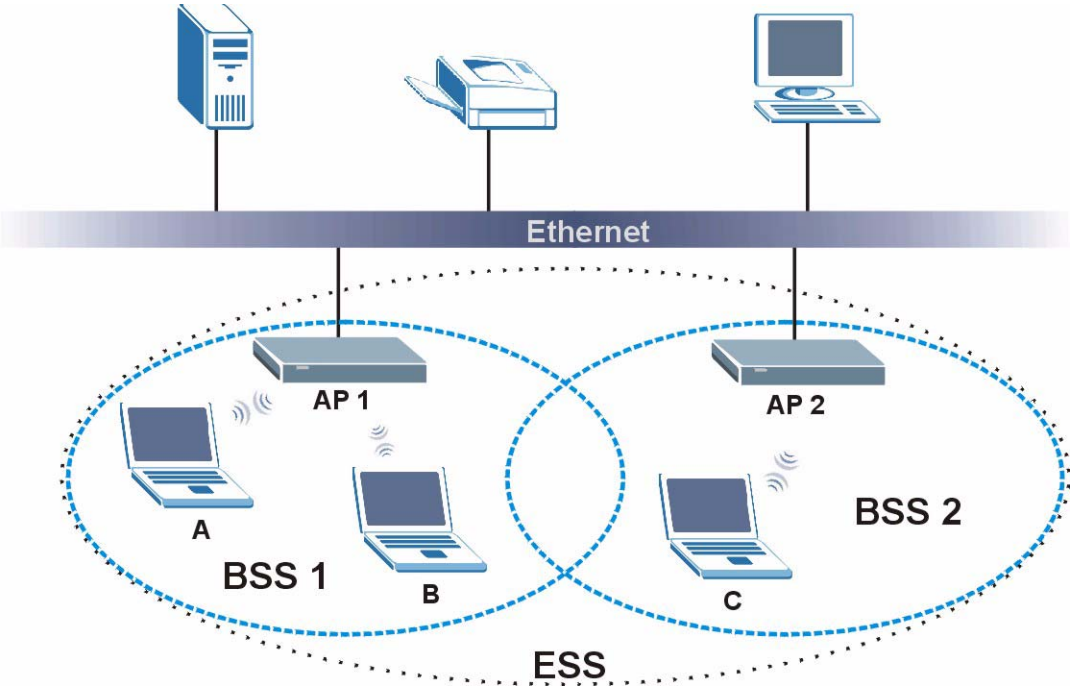
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 370 Infrastructure WLAN



Channel

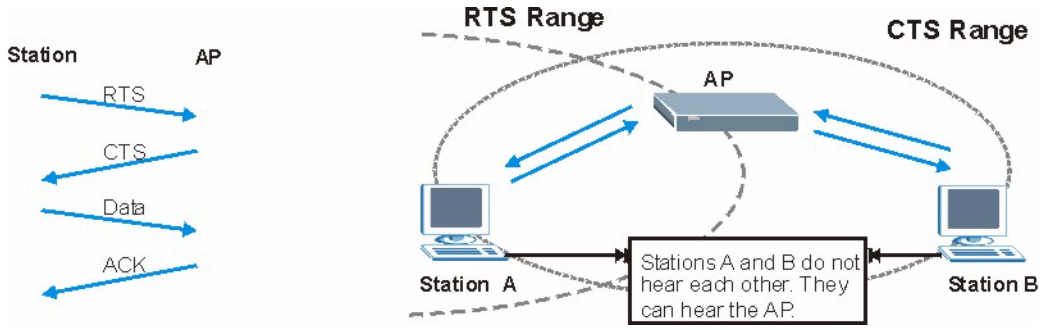
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 371 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.

The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 193 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 194 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting
  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
  Sent by an access point requesting authentication.
- Access-Reject
  Sent by a RADIUS server rejecting access.
- Access-Accept
  Sent by a RADIUS server allowing access.
- Access-Challenge
  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
  Sent by the access point requesting accounting.
- Accounting-Response
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 195 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

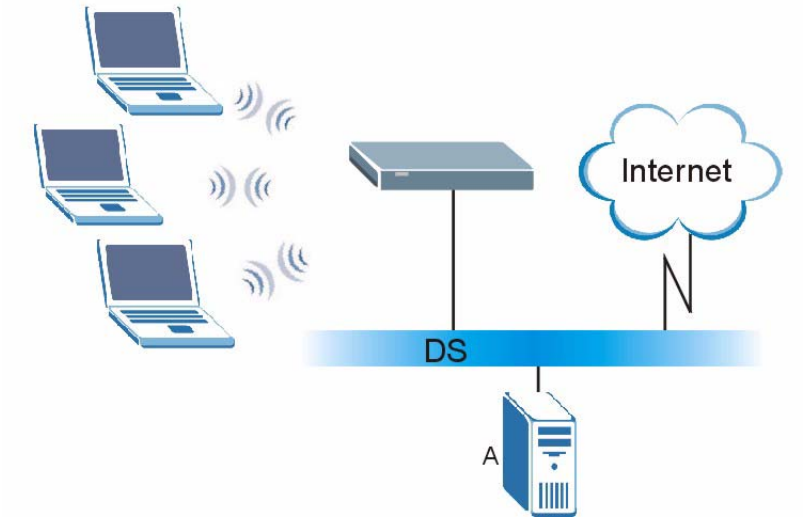
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 372 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

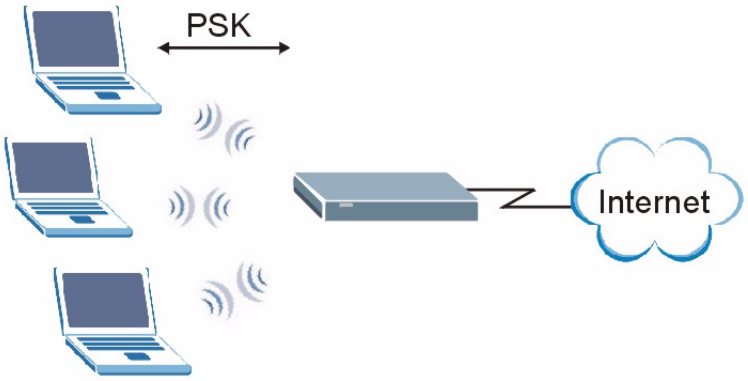
A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 373 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 196 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 197 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.

Table 197 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.

Table 197 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 197 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

F

Internal SPTGEN

Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple ZyXEL Devices. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual screens for each ZyXEL Device.

The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values allowed =
input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

Figure 374 Configuration Text File Format: Column Descriptions

```
/ Menu 1 General Setup
 10000000 = Configured                <0(No)| 1(Yes)>       = 1
 10000001 = System Name               <Str>                 = Your Device
 10000002 = Location                  <Str>                 =
 10000003 = Contact Person's Name     <Str>                 =
 10000004 = Route IP                  <0(No)| 1(Yes)>       = 1
 10000005 = Route IPX                <0(No)| 1(Yes)>       = 0
 10000006 = Bridge                   <0(No)| 1(Yes)>       = 0
```

DO NOT alter or delete any field except parameters in the Input column.

This appendix introduces Internal SPTGEN. All menus shown in this appendix are example menus meant to show SPTGEN usage. Actual menus for your product may differ.

Internal SPTGEN File Modification - Important Points to Remember

Each parameter you enter must be preceded by one "="sign and one space.

Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see Figure 374 on page 503), then you disable every field in this menu.

If you enter a parameter that is invalid in the **Input** column, the ZyXEL Device will not save the configuration and the command line will display the **Field Identification Number**. Figure 375 on page 504, shown next, is an example of what the ZyXEL Device displays if you enter a value other than "0" or "1" in the **Input** column of **Field Identification Number** 1000000 (refer to Figure 374 on page 503).

Figure 375 Invalid Parameter Entered: Command Line Example

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

The ZyXEL Device will display the following if you enter parameter(s) that *are* valid.

Figure 376 Valid Parameter Entered: Command Line Example

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Internal SPTGEN FTP Download Example

1. Launch your FTP application.
2. Enter "`bin`". The command "`bin`" sets the transfer mode to binary.
3. Get "`rom-t`" file. The command "`get`" transfers files from the ZyXEL Device to your computer. The name "`rom-t`" is the configuration filename on the ZyXEL Device.
4. Edit the "`rom-t`" file using a text editor (do not use a word processor). You must leave this FTP screen to edit.

Figure 377 Internal SPTGEN FTP Download Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

You can rename your "rom-t" file when you save it to your computer but it must be named "rom-t" when you upload it to your ZyXEL Device.

Internal SPTGEN FTP Upload Example

1. Launch your FTP application.
2. Enter "bin". The command "bin" sets the transfer mode to binary.
3. Upload your "rom-t" file from your computer to the ZyXEL Device using the "put" command. computer to the ZyXEL Device.
4. Exit this FTP application.

Figure 378 Internal SPTGEN FTP Upload Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Example Internal SPTGEN Screens

This section covers ZyXEL Device Internal SPTGEN screens.

Table 198 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number
FN	Field Name

Table 198 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the ZyXEL Device.

The following are the Internal SPTGEN menus.

Table 199 Menu 1 General Setup

/ Menu 1 General Setup			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0(No) | 1(Yes)>	= 0
10000001 =	System Name	<Str>	= Your Device
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0(No) | 1(Yes)>	= 1
10000006 =	Bridge	<0(No) | 1(Yes)>	= 0

Table 200 Menu 3

/ Menu 3.1 General Ethernet Setup			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ Menu 3.2 TCP/IP and DHCP Ethernet Setup			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0(None) | 1(Server) | 2(Relay)>	= 0

Table 200 Menu 3

30200002 =	Client IP Pool Starting Address		= 192.168.1.33
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0
30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30200011 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30200012 =	Multicast	<0(IGMP-v2) | 1(IGMP-v1) | 2(None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ Menu 3.2.1 IP Alias Setup			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0(No) | 1(Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30201005 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256

Table 200 Menu 3

30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256
30201014 =	IP Alias 2 <0(No) | 1(Yes)>		= 0
30201015 =	IP Address		= 0.0.0.0
30201016 =	IP Subnet Mask		= 0
30201017 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30201018 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256
*/ Menu 3.5 Wireless LAN Setup			
FIN	FN	PVA	INPUT
30500001 =	ESSID		Wireless
30500002 =	Hide ESSID	<0(No) | 1(Yes)>	= 0
30500003 =	Channel ID	<1|2|3|4|5|6|7|8|9|10|11|12|13>	= 1
30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0(DISABLE) | 1(64-bit WEP) | 2(128-bit WEP)>	= 0

Table 200 Menu 3

30500007 =	Default Key	<1|2|3|4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=
30500011 =	WEP Key4		=
30500012 =	Wlan Active	<0(Disable) | 1(Enable)>	= 0
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER			
FIN	FN	PVA	INPUT
30501001 =	Mac Filter Active	<0(No) | 1(Yes)>	= 0
30501002 =	Filter Action	<0(Allow) | 1(Deny)>	= 0
30501003 =	Address 1		= 00:00:00:00:00:00
30501004 =	Address 2		= 00:00:00:00:00:00
30501005 =	Address 3		= 00:00:00:00:00:00
Continued	…		…
30501034 =	Address 32		= 00:00:00:00:00:00

Table 201 Menu 4 Internet Access Setup

/ Menu 4 Internet Access Setup			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0(No) | 1(Yes)>	= 1
40000001 =	ISP	<0(No) | 1(Yes)>	= 1
40000002 =	Active	<0(No) | 1(Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1(LLC-based) | 2(VC-based)	= 1

Table 201 Menu 4 Internet Access Setup (continued)

40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0(No) | 1(Yes)>	= 1
40000012 =	IP Address Assignment	<0(Static)|1(Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0(No) | 1(Yes)>	= 1
40000026 =	Bridge	<0(No) | 1(Yes)>	= 0
40000027 =	ATM QoS Type	<0(CBR) | (1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size(MBS)		= 0
40000031=	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0(No) |1(Yes)>	= 0

Table 202 Menu 12

/ Menu 12.1.1 IP Static Route Setup			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0(No) |1(Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0(No) |1(Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0(No) |1(Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.4 IP Static Route Setup			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0(No) |1(Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0

Table 202 Menu 12 (continued)

120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0(No) |1(Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0(No) |1(Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0(No) |1(Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.8 IP Static Route Setup			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(No) |1(Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0

Table 202 Menu 12 (continued)

120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.9 IP Static Route Setup			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(No) |1(Yes)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.10 IP Static Route Setup			
FIN	FN	PVA	INPUT
120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(No) |1(Yes)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask		= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric		= 0
120110007 =	IP Static Route set #10, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.11 IP Static Route Setup			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(No) |1(Yes)>	= 0
120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0
120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.12 IP Static Route Setup			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0(No) |1(Yes)>	= 0

Table 202 Menu 12 (continued)

120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.13 IP Static Route Setup			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name	<Str>	=
120113002 =	IP Static Route set #13, Active	<0(No) |1(Yes)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.14 IP Static Route Setup			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0(No) |1(Yes)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.15 IP Static Route Setup			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=
120115002 =	IP Static Route set #15, Active	<0(No) |1(Yes)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.16 IP Static Route Setup			
FIN	FN	PVA	INPUT

Table 202 Menu 12 (continued)

120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0(No) |1(Yes)>	= 0
120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0(No) |1(Yes)>	= 0

Table 203 Menu 15 SUA Server Setup

/ Menu 15 SUA Server Setup			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0(No) | 1(Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0(No) | 1(Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0(No) | 1(Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0(No) | 1(Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0(No) | 1(Yes)> = 0	= 0

Table 203 Menu 15 SUA Server Setup (continued)

150000023 =	SUA Server #6 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0(No) | 1(Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0(No) | 1(Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0(No) | 1(Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042	= SUA Server #10 Active	<0(No) | 1(Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0(No) | 1(Yes)>	= 0
150000048 =	SUA Server #11 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0(No) | 1(Yes)>	= 0
150000053 =	SUA Server #12 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0

Table 204 Menu 21.1 Filter Set #1

/ Menu 21 Filter set #1			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 set #1, rule #1			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type	<2(TCP/IP)>	= 2
210101002 =	IP Filter Set 1,Rule 1 Active	<0(No)|1(Yes)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.2 set #1, rule #2			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0(No)|1(Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0

Table 204 Menu 21.1 Filter Set #1 (continued)

210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.3 set #1, rule #3			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2(TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0(No)|1(Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match	<1(check next)|2(forward)|3(drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0(No)|1(Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0

Table 204 Menu 21.1 Filter Set #1 (continued)

210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1(check next)|2(forward) | 3(drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2(TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0(No)|1(Yes)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1(Check Next)|2(Forward)|3(Drop)>	= 1

Table 204 Menu 21.1 Filter Set #1 (continued)

/ Menu 21.1.1.6 set #1, rule #6			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0(No)|1(Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2

Table 205 Menu 21.1 Filer Set #2,

/ Menu 21.1 filter set #2,			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN
/ Menu 21.1.2.1 Filter set #2, rule #1			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0(none)|2(TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0(No)|1(Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137

Table 205 Menu 21.1 Filer Set #2, (continued)

210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2, Rule 2 Type	<0(none)|2(TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0(No)|1(Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2,Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3

Table 205 Menu 21.1 Filer Set #2, (continued)

210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.3 Filter set #2, rule #3			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0(none)|2(TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0(No)|1(Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2,Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210203014 =	IP Filter Set 2,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0(none)|2(TCP/IP)>	= 2
210204002 =	IP Filter Set 2, Rule 4 Active		<0(No)|1(Yes)> = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137

Table 205 Menu 21.1 Filer Set #2, (continued)

210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0(none)|2(TCP/IP)>	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0(No)|1(Yes)>	= 1
210205003 =	IP Filter Set 2,Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0
210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3

Table 205 Menu 21.1 Filer Set #2, (continued)

210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0(none)|2(TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0(No)|1(Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210206013 =	IP Filter Set 2,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210206014 =	IP Filter Set 2,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2
241100005 =	FTP Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(all)|1(none)|2(Lan) |3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

Table 206 Menu 23 System Menus

*/ Menu 23.1 System Password Setup			
FIN	FN	PVA	INPUT

Table 206 Menu 23 System Menus (continued)

230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured	<0(No) | 1(Yes)>	= 1
230200002 =	Authentication Server Active	<0(No) | 1(Yes)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822
230200005 =	Authentication Server Shared Secret		= 111111111111111 111111111111111
230200006 =	Accounting Server Configured	<0(No) | 1(Yes)>	= 1
230200007 =	Accounting Server Active	<0(No) | 1(Yes)>	= 1
230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
*/ Menu 23.4 System security: IEEE802.1x			
FIN	FN	PVA	INPUT
230400001 =	Wireless Port Control	<0(Authentication Required) |1(No Access Allowed) |2(No Authentication Required)>	= 2
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0(Local User Database Only) |1(RADIUS Only) |2(Local,RADIUS) |3(RADIUS,Local)>	= 1
230400005 =	Key Management Protocol	<0(8021x) |1(WPA) |2(WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange	<0(Disable) |1(64-bit WEP) |2(128-bit WEP)>	= 0
230400007 =	PSK =		=
230400008 =	WPA Mixed Mode	<0(Disable) |1(Enable)>	= 0
230400009 =	Data Privacy for Broadcast/ Multicast packets	<0(TKIP) |1(WEP)>	= 0
230400010 =	WPA Broadcast/Multicast Key Update Timer		= 0

Table 207 Menu 24.11 Remote Management Control

/ Menu 24.11 Remote Management Control			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(all)|1(none)|2(Lan) |3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

Command Examples

The following are example Internal SPTGEN screens associated with the ZyXEL Device's command interpreter commands.

Table 208 Command Examples

FIN	FN	PVA	INPUT
/ci command (for annex a): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(glite)|1(t1.413)|2(gdmt)|3(multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(etsi)|1(normal)|2(gdmt)|3(multimode)>	= 3

G

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

H

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: ftp.us.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

A

AAL5 436
ACK message 189
adding a printer example 365
adding a printer example, Macintosh OS 370
Address Resolution Protocol (ARP) 147
ADSL2 436
Advanced Encryption Standard
  See AES.
AES 494
AH 267
AH protocol 271
ALG 184, 439
alternative subnet mask notation 479
antenna 433
  directional 497
  gain 497
  omni-directional 497
any IP 146, 435
  how it works 147
  note 147
any IP setup 149
AP (access point) 487
Application Layer Gateway 184, 439
applications
  Internet access 45
Asynchronous Transfer Mode 422
ATC 325
ATM AAL5 436
ATM Adaptation Layer 5 (AAL5) 128, 436
attack alert 258
authentication header 271
auto attendant, and VoIP trunking 225
auto dial 438
auto firmware upgrade 238
auto provisioning 238
Automatic Traffic Classifier
  see ATC
auto-negotiating rate adaptation 436
auto-provisioning 238

B

backup 413
backup type 141
bandwidth management 325
bandwidth manager class configuration 328
bandwidth manager monitor 332
bandwidth manager summary 327
base station
  DECT 202
Basic Service Set, See BSS 485
basic wireless security 102
blinking LEDs 48
browsing, to a file share 385, 386
BSS 485
BW budget 329
BYE request 189

C

CA 492
CA (Certification Authority) 297
call fallback 438
call forwarding 439
call hold 210, 211
call park and pickup 438
call return 438
call rules, and VoIP trunking 223
call service mode 209, 211
call transfer 210, 211
call waiting 210, 211, 438
caller ID 439
CBR (Continuous Bit Rate) 134, 139
CCK 441
certificate
  details 304
  factory default 299
Certificate Authority
  See CA.
certificates 297
  advantages 298
  and cryptology 297
  and directory servers 298, 318

and public-key cryptology 297
and public-private keys 297
and remote hosts 312
creating 302
file formats 301
generating requests 297
importing 300
remote hosts 315
replacing 299
revoked 298
storage space 299
trusted CAs 307, 309
verifying 314
Certification Authority (CA) 297
certifications 527
notices 528
viewing 528
channel 487
interference 487
channel ID 160
CIFS (Common Internet File System) 378
Class of Service 192
client-server protocol 186
codecs 439
comfort noise generation 200, 439
Common Internet File System (CIFS) 378
Complementary Code Keying Modulation 441
configuration 143
configuration file 409
contact information 531
content filtering 261, 435
categories 261
schedule 262
trusted computers 263
URL keyword blocking 261
copyright 527
CoS 192
country code 438
creating certificates 302
CTS (Clear to Send) 488
custom ports
creating/editing 252
customer support 531
customized services 252

D

data confidentiality 266
data integrity 266
data origin authentication 266
DBPSK 441
DECT 202
and flashing 206
and PIN for registration 204
and PSTN 206
and SIP 206
and supplementary services 206
and VoIP 206
base station 202
base station button 203
base station reset 205
external calls 206
handset 203
internal calls 206
phone registration 203
phone usage 205
security 204
SIP line assignment 207
web configurator 206
DECT (Digital Enhanced Cordless Telecommunications) 47
default 414
default LAN IP address 81
DH 285
DHCP 143, 144, 333, 391, 436
DHCP client 436
DHCP relay 436
DHCP server 436
diagnostic 421
Differential Binary Phase Shift Keyed Modulation 441
Differential Quadrature Phase Shift Keying Modulation 441
differentiated services 193
Diffie-Hellman key groups 285
DiffServ 192
DiffServ code points 192
DiffServ marking rule 193
Digital Enhanced Cordless Telecommunications, See DECT 47
directory servers
adding/editing 319
certificates 298
directory servers, and certificates 318
disclaimer 527
distinctive ring 216, 438
DnD 438
DNS 144, 344
DNS Server
for VPN host 276
do not disturb 438
domain name 391
domain name system
see DNS
DoS 259

DoS (Denial of Service) 435
DQPSK 441
DS field 193
DSCPs 192
DSL line, reinitialize 423
DTMF 191
DTMF detection and generation 439
Dual-Tone MultiFrequency 191
dynamic DNS 333, 435
Dynamic Host Configuration Protocol 436
dynamic jitter buffer 439
dynamic secure gateway address 273
dynamic WEP key exchange 493
DYNDNS wildcard 333

E

EAP Authentication 491
EAP-MD5 440
echo cancellation 200, 439
e-mail 172
  log example 399
emergency numbers 218
encapsulated routing link protocol (ENET ENCAP) 127
encapsulation 127, 267
  ENET ENCAP 127
  PPP over Ethernet 127
  PPPoA 128
  RFC 1483 128
encapsulation security payload 271
encryption 265, 494
ESP 267
ESP protocol 271
ESS 486
ETSI (European Telecommunications Standards Institute) 202
Europe type call service mode 209
Extended Service Set IDentification 159
Extended Service Set, See ESS 486
extended wireless security 102
external antenna 440
external RADIUS 440

F

F4/F5 OAM 436
FAT (File Allocation Table) 377
FCC interference statement 527
File Allocation Table, see FAT 377
file sharing 47, 377, 378
  and workgroup 378, 387
  overview 377
  user account 379
  web configurator 379, 380, 381, 382
  Windows Explorer 385, 386
filename conventions 409, 410
Firewall 241, 242
firewall
  address type 251
  creating/editing rules 249
  custom ports 252
  DoS 259
  Dos threshold 259
  enabling 246
  maximum incomplete high 259
  maximum incomplete low 259
  one minute high 259
  one minute low 259
  policies 242
  rule security considerations 244
  stateful inspection 242
  TCP maximum incomplete 259
  three-way handshake 257
firmware 410
  upload 410
  upload error 412
firmware upgrade 238
flash key 209
flashing 209
  and DECT phones 206
fragmentation threshold 488
frequency range 440
FTP 178, 340
  file upload 419
FTP restrictions 410

G

G.168 200, 439
G.711 439
G.726 439
G.729 439
G.992.1 436
G.992.3 436
G.992.4 436
G.992.5 436
GAP 47
GAP (Generic Access Profile) 203

general setup 391
Generic Access Profile, see GAP 203
group ring 216, 438

H

hidden node 487
host 392
HTTP (Hypertext Transfer Protocol) 410
HTTP pincode 238
humidity 433

I

IANA 145, 484
  Internet Assigned Numbers Authority
    see IANA
IANA (Internet Assigned Number Authority) 252
IBSS 485
ID type and content 277
IEEE 802.11g 440, 441, 489
IEEE 802.11g data rates 441
IEEE 802.11g modulation 441
IEEE 802.11g wireless LAN 440
IEEE 802.11i 440
IEEE 802.1Q VLAN 193
IGMP 146
IGMP proxy 436
IGMP v1 436
IGMP v2 436
IKE phases 284
importing certificates 300
importing trusted CAs 309
importing trusted remote hosts 315
Independent Basic Service Set
  See IBSS 485
initialization vector (IV) 494
inside header 268
install UPnP 349
  Windows Me 349
  Windows XP 350
Integrated Access Device 43
Integrated Services Digital Network 44
internal calls 237, 438
internal SPTGEN 503
  FTP upload example 505
  points to remember 504
  text file 503
Internet access 45, 91
Internet access wizard setup 91
Internet Assigned Numbers Authority
  See IANA
Internet Key Exchange 284
Internet Protocol Security 265
IP address 144, 178, 179, 180, 238
IP address assignment 128
  ENET ENCAP 129
  PPPoA or PPPoE 129
  RFC 1483 129
IP alias 436
IP multicasting 436
IP network and PSTN connection 221
IP pool 150
IP pool setup 144
IPSec 265
IPSec algorithms 267, 271
IPSec and NAT 268
IPSec architecture 266
IPSec passthrough 437
IPSec standard 435
IPSec VPN capability 435
ISDN (Integrated Services Digital Network) 44
ITU-T 200
ITU-T G.992.1 423

J

jitter buffer 439

K

keep alive 275
key combinations 238
keypad 238
keys and certificates 297

L

LAN
  and USB printer 359
LAN setup 127, 143
LAN TCP/IP 144

listening port 198
log out 83
log out (automatic) 83
logs 395

M

MAC address filter action 169
MAC filter 168
Management Information Base (MIB) 342
managing the device
  good habits 44
  using FTP. See FTP.
  using Telnet. See command interface.
  using the command interface. See command interface.
Maximum Burst Size (MBS) 130, 135, 140
maximum incomplete high 259
maximum incomplete low 259
media bandwidth management 435
Message Integrity Check (MIC) 494
metric 129
multicast 146
multimedia 185
multiple PVC support 436
multiple SIP accounts 439
multiple voice channels 439
multiplexing 128
  LLC-based 128
  VC-based 128
multiprotocol encapsulation 128
music on hold 438
my IP address 272

N

nailed-up connection 129
NAT 145, 178, 179, 435, 484
  address mapping rule 182
  application 175
  definitions 173
  how it works 174
  mapping types 175
  what it does 174
NAT (Network Address Translation) 173
NAT mode 177
NAT sessions 437
NAT traversal 276, 347
negotiation mode 285
Network Address Translation
  see NAT

O

OAM 436
OFDM 441
OK response 189, 190
one minute high 259
one minute low 259
operation humidity 433
operation temperature 433
Orthogonal Frequency Division Multiplexing Modulation 441
outside header 268

P

Pairwise Master Key (PMK) 494, 496
park 438
password change at login 82
Peak Cell Rate (PCR) 130, 134, 139
peer call authentication, VoIP trunking 222
peer IP 227
peer port 227
peer-to-peer calls 46
Perfect Forward Secrecy 285
per-hop behavior 193
Permanent Virtual Circuits 436
Personal Identification Number, see PIN 204
PFS 285
PHB (Per-Hop Behavior) 193
phone 199
phone config 438
phone functions 238
pickup 438
PIN (Personal Identification Number) 204
PIN, and DECT phone 204
pincode 238
PKI (Public-Key Infrastructure) 298
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) 128
point-to-point calls 439
port forwarding 437
ports 48

power adaptor 441
power specifications 433
PPP (Point-to-Point Protocol) Link Layer Protocol 436
PPP over ATM AAL5 436
PPP over Ethernet 436
PPPoE 127
  benefits 127
PPPoE (Point-to-Point Protocol over Ethernet) 127, 435
preamble mode 489
pre-shared key 279
print server 47
printer sharing 359
  and LAN 359
  configuration 360
  requirements 359
  TCP/IP port 360
  web configurator 364
priorities 327
priority 329
product registration 529
PSK 494
PSTN
  and DECT 206
PSTN call setup signaling 191
Public Switched Telephone Network 43
public-key cryptology, and certificates 297
public-private keys
  and certificates 297
pulse dialing 191
PVCs 436

Q

QoS 192, 439
Quality of Service 192, 439
quick dialing 439
Quick Start Guide 81

R

RADIUS 440, 490
  message types 491
  messages 491
  shared secret key 491
Reach-Extended ADSL 436
Real time Transport Protocol 188
real-time e-mail alerts 437
region 438
registration
  product 529
reinitialize the ADSL line 423
related documentation 3
remote hosts, and certificates 312
remote management
  Telnet 339
remote management and NAT 338
remote management limitations 338
REN 439
reports and logs 437
resetting your device 49
restore 413
restore configuration 418
RF (Radio Frequency) 441
RFC 1483 128, 436
RFC 1631 173
RFC 1889 188, 439
RFC 1890 439
RFC 2327 439
RFC 2364 436
RFC 2516 435, 436
RFC 2684 436
RFC 3261 439
Ringer Equivalence Number 439
ringing 438
RIP 145
  direction 145
  Routing Information Protocol
    see RIP
  version 146
romfile 409
router features 45
RTCP 439
RTP 188, 439
RTS (Request To Send) 488
  threshold 487, 488

S

SA 265
safety warnings 6
SDP 439
seamless rate adaptation 436
secure gateway address 272
security
  and certificates 297
  DECT phone 204

security association 265
Security Parameter Index 288
server 176, 394
Service Set 159
service type 253
services 178
Session Description Protocol 439
Session Initiating Protocol 439
Session Initiation Protocol 185
setup 238
sharing files 378
silence suppression 199, 439
SIP 185
  and DECT 206
SIP account 185
SIP accounts 439
SIP ALG 184, 439
SIP ALG passthrough 437
SIP Application Layer Gateway 184, 439
SIP authentication password 107
SIP authentication user ID 107
SIP call progression 188
SIP client 186
SIP identities 185
SIP INVITE request 189, 190
SIP number 107, 185
SIP OK response 190
SIP proxy server 187
SIP redirect server 187
SIP register server 188
SIP server address 107
SIP servers 186
SIP service domain 107, 186
SIP URI 185
SIP user agent 186
SIP version 2 439
SMTP error messages 398
SNMP 341, 436
  manager 342
  MIBs 342
speed dial 213, 237
SPI 288
SRA 436
Stateful Inspection 241
stateful inspection 435
stateful inspection firewall 242
stateful packet inspection 437
static route 321
status indicators 48
storage humidity 433
storage temperature 433
SUA 176
SUA (Single User Account) 176
SUA vs NAT 176
subnet 477
subnet mask 144, 251, 478
subnetting 480
supplementary services 209
  and DECT phones 206
Sustain Cell Rate (SCR) 135, 139
Sustained Cell Rate (SCR) 130
syntax conventions 4
syslog 256
system name 392
System Parameter Table Generator 503
system timeout 338

T

TCP maximum incomplete 258, 259
TCP/IP port 360
Telnet 339
temperature 433
Temporal Key Integrity Protocol (TKIP) 494
TFTP
  file upload 420
TFTP and FTP over WAN 410
three-way conference 210, 211
TLS 440
ToS 192
trademarks 527
traffic redirect 140, 142
traffic shaping 130
transparent bridging 436
transport mode 268
Triangle 245
Triangle Route Solutions 245
trunking 439
trunking, VoIP 221
trusted CAs, and certificates 307
TTLS 440
tunnel mode 268
Type of Service 192

U

UBR (Unspecified Bit Rate) 134, 139
Uniform Resource Identifier 185
Universal Plug and Play 347
  application 347
Universal Plug and Play (UPnP) 435
upload firmware 418
UPnP 347
  forum 348
  security issues 347
USA type call service mode 211
USB
  and file sharing 377
  hard drive 377
  printer sharing 359
USB features 47
USB printer 47

V

VAD 199, 439
VBR (Variable Bit Rate) 139
VBR-nRT 134
VBR-RT 134
Virtual Channel Identifier (VCI) 128
Virtual Circuit (VC) 128
Virtual Local Area Network 193
Virtual Path Identifier (VPI) 128
Virtual Private Network 43, 265, 435
VLAN 193
VLAN group 193
VLAN ID 193
VLAN ID tags 193
voice activity detection 199, 439
voice channels 439
voice coding 190
VoIP 185
  and DECT 206
  ring selection 216
  testing rings 217
VoIP features 46
VoIP links 221
VoIP standards compliance 439
VoIP trunking 46, 221
  and security 221
  call rules 223
  detailed example 229, 230, 231, 232, 234
  examples 223, 224
  how it works 221
  overview 221
  peer authentication 226
  peer calls 225
  scenarios 223, 224
  SIP settings 224
  web configurator 224
VPI & VCI 128
VPN 265
VPN applications 266

W

WAN (Wide Area Network) 127
warranty 529
  note 529
Web 338
Web Configurator 81, 244
  and VoIP trunking 224
web configurator
  and DECT phone 206
WEP (Wired Equivalent Privacy) 440
WEP encryption 162
Wi-Fi Protected Access 493
Wi-Fi Protected Access (WPA) 440
Windows Explorer, and file sharing 385, 386
wireless client WPA supplicants 495
wireless LAN MAC address filtering 440
wireless security 489
Wireless tutorial 51
WLAN
  interference 487
  security parameters 496
WLAN button 50
workgroup, and file sharing 378, 387
WPA 493
  key caching 494
  pre-authentication 494
  user authentication 494
  vs WPA-PSK 494
  wireless client supplicant 495
  with RADIUS application example 495
WPA2 493
  user authentication 494
  vs WPA2-PSK 494
  wireless client supplicant 495
  with RADIUS application example 495
WPA2-Pre-Shared Key 493
WPA2-PSK 493, 494
  application example 495
WPA-PSK 493, 494
  application example 495

WWW 172

Z

zero configuration Internet access 131, 435
ZyNOS 410
ZyNOS (ZyXEL Network Operating System) 410
ZyNOS F/W version 410